NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27002 2022

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 15046) Lima, Perú

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

Information security, cybersecurity and privacy protection. Information security controls

(EQV. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls)

2022-12-29
2ª Edición

R.D. N° 022-2022-INACAL/DN. Publicada el 2023-01-12 Precio basado en 291 páginas
I.C.S.: 35.030 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología de la información, seguridad, controles de seguridad

INACAL

Calle Las Camelias 817, San Isidro
Lima - Perú
Tel.: +51 1 640-8820
publicaciones@inacal.gob.pe
www.inacal.gob.pe

ÍNDICE

página

PRÓLOGO

A. RESEÑA HISTÓRICA

A.1 El Instituto Nacional de Calidad - INACAL, a través de la Dirección de Normalización es la autoridad competente que aprueba las Normas Técnicas Peruanas a nivel nacional. Es miembro de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en representación del país.

A.2 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de marzo a octubre de 2022, utilizando como antecedente a la norma ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls.

A.3 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Dirección de Normalización -DN-, con fecha 2021-10-11, el PNTP-ISO/IEC 27002:2022 para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2022-10-28. Habiéndose recibido observación, esta fue revisada y luego de su evaluación correspondiente, fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información**, 2ª Edición, el 12 de enero de 2023.

A.4 Esta segunda edición de la NTP-ISO/IEC 27002 reemplaza a la NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información, 1ª Edición. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurado de acuerdo a las Guías Peruanas GP 001:2016 y GP 002:2016.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría	GS1 Perú
Presidente	Carlos Horna Vallejos

Secretaria	Mary Wong Suehiro

ENTIDAD	**REPRESENTANTE**
Criptografía Legal S. A. C.	Nataly Bravo López Isbert Panez Wuchenauer
GS1 PERÚ	Paola Carhuatanta
IBM del Perú S. A. C.	Iván Ancco Peña
Indecopi - Gerencia de Planeamiento y Gestión Institucional	César Guerra Camargo
Ministerio de Economía y Finanzas – Dirección General de Asuntos de Economía Internacional, Competencia y Productividad	Luzmila Zegarra Valencia
Secretaría de Gobierno Digital – PCM	Carlos Arias Ramos
SUNAT	Daniel Llanos Panduro
Consultor	Gustavo Vallejo La Torre
Consultor	Marco Bermúdez Torres

PRÓLOGO
(ISO/IEC)

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado de normalización mundial. Los organismos nacionales miembros de ISO o IEC participan en la elaboración de normas internacionales a través de comités técnicos creados por la organización respectiva para ocuparse de determinados campos de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también participan en los trabajos.

Los procedimientos utilizados para desarrollar este documento y los destinados a su posterior mantenimiento se describen en las Directivas ISO/IEC, Parte 1. En particular, debería tenerse en cuenta los diferentes criterios de aprobación necesarios para los distintos tipos de documentos. Este documento se ha redactado de acuerdo con las normas de redacción de las Directivas ISO/IEC, Parte 2 (véase www.iso.org/directives o www.iec.ch/members_experts/refdocs).

Se presta atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no deben responsabilizarse de la identificación de ninguno o de todos esos derechos de patente. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento aparecerán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (véase www.iso.org/patents) o en la lista IEC de declaraciones de patentes recibidas (véase patents.iec.ch).

Cualquier nombre comercial utilizado en este documento es una información que se ofrece para comodidad de los usuarios y no constituye una aprobación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html. En IEC, véase www.iec.ch/understanding-standards.

Este documento ha sido elaborado por el Comité Técnico Conjunto *ISO/IEC JTC 1, Tecnología de la Información*, Subcomité SC 27, *Seguridad de la información, ciberseguridad y protección de la privacidad.*

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

Los principales cambios son los siguientes

- se ha modificado el título;
- se ha cambiado la estructura del documento, presentando los controles mediante una taxonomía simple y atributos asociados;
- se han fusionado algunos controles, se han eliminado otros y se han introducido varios controles nuevos. La correspondencia completa se encuentra en el Anexo B.

Cualquier comentario o pregunta sobre este documento debería dirigirse al organismo nacional de normalización del usuario. La lista completa de estos organismos puede encontrarse en www.iso.org/members.html y www.iec.ch/national-committees.

INTRODUCCIÓN

0.1 Antecedentes y contexto

Este documento está diseñado para organizaciones de todo tipo y tamaño. debería utilizarse como una referencia para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información en un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001. También puede utilizarse como un documento de orientación para las organizaciones que determinan e implementan controles de seguridad de la información comúnmente aceptados. Además, este documento está destinado para ser utilizado en el desarrollo de lineamientos en gestión de seguridad de la información para la industria y de una organización específica, tomando en consideración su entorno(s) de riesgo de seguridad de la información específicos. Los controles específicos para la organización o el entorno específico distintos de los incluidos en este documento pueden ser determinados a través de la evaluación de riesgos según sea necesario.

Las organizaciones de todo tipo y tamaño (incluidos el sector público y privado, comerciales y sin fines de lucro) crean, recopilan, procesan, almacenan, transmiten y eliminan información en muchas formas, incluyendo la electrónica, física y verbal (por ejemplo, conversaciones y presentaciones).

El valor de la información va más allá de las palabras escritas, los números e 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 adecuado conjunto 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 ISO/IEC 27001 adopta una visión holística y coordinada de los riesgos de seguridad de la información de la organización para determinar e implementar un conjunto completo de controles de seguridad de la información dentro del marco de trabajo de un sistema de gestión coherente.

Muchos sistemas de información, incluida su gestión y operaciones, no han sido diseñados para ser seguros en términos de un SGSI como se especifica en ISO/IEC 27001 y en este documento. El nivel de seguridad que se puede alcanzar solo mediante medidas tecnológicas es limitado y debería estar respaldado por actividades de gestión y procesos organizativos adecuados. La identificación de los controles que se deberían implementar requiere una planificación cuidadosa y atención a los detalles al llevar a cabo el tratamiento de riesgos.

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

Un sistema de gestión de seguridad de la información conveniente, adecuado y eficaz proporciona garantía 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 de negocio establecidos.

0.2 Requisitos de seguridad de la información

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

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

b) los requisitos legales, estatutarios, ´ y contractuales que una organización y sus partes interesadas (socios comerciales, proveedores de servicios, entre otros) tienen que cumplir y su entorno sociocultural;

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

0.3 Controles

Un control se define como una medida que modifica o mantiene el riesgo. Algunos de los controles en este documento son controles que modifican el riesgo, mientras que otros mantienen el riesgo. Una política de seguridad de la información, por ejemplo, solo puede mantener el riesgo, mientras que el cumplimiento de dicha política de seguridad de la información puede modificar el riesgo.

Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo. Este documento proporciona una combinación genérica de controles de seguridad de la información organizativos, de personas, físicos y tecnológicos derivados de las mejores prácticas reconocidas internacionalmente.

0.4 Determinación de controles

La determinación de los controles depende de las decisiones de la organización después de una evaluación de riesgos, con un alcance claramente definido. Las decisiones relacionadas con los riesgos identificados deberían basarse en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque de gestión del riesgo aplicado por la organización. La determinación de los controles también debería tomar en consideración todas las leyes y regulaciones nacionales e internacionales relevantes. La determinación del control también depende de la manera en que los controles interactúan entre sí para proporcionar una defensa en profundidad.

La organización puede diseñar controles según lo requiera o identificarlos desde cualquier fuente. Al especificar dichos controles, la organización debería considerar los recursos y la inversión necesarios para implementar y operar un control contra el valor de negocio obtenido. Consulte ISO/IEC TR 27016 para obtener orientación sobre las decisiones relacionadas con la inversión en un SGSI y las consecuencias económicas de estas decisiones en el contexto de la competencia por recursos requeridos.

Debería haber un equilibrio entre los recursos desplegados para implementar controles y el potencial impacto en el negocio resultante de los incidentes de seguridad en ausencia de estos controles. Los resultados de una evaluación de riesgos deberían ayudar a guiar y determinar la acción de gestión adecuada, las prioridades para gestionar los riesgos de seguridad de la información y para implementar los controles que se determinen como necesarios para protegerse contra estos riesgos.

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

0.5 Desarrollar lineamientos específicos para la organización

Este documento puede considerarse como un punto de partida para desarrollar lineamientos específicos para la organización. No todos los controles y orientación en este documento pueden aplicarse a todas las organizaciones. También se pueden requerir controles y lineamientos adicionales no incluidos en este documento para abordar las necesidades específicas de la organización y los riesgos que se han identificado.

Cuando se desarrollan documentos que contienen lineamientos o controles adicionales, puede ser útil incluir referencias cruzadas a capítulos de este documento 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 de, y los riesgos para la información pueden variar a lo largo de este ciclo de vida (por ejemplo, la divulgación no autorizada o el robo de las cuentas financieras de una empresa no es significativo después de que esta fuera publicada, pero la integridad sigue siendo crítica) por lo tanto, la seguridad de la información sigue siendo importante hasta cierto punto en todas las etapas.

Los sistemas de información y otros activos relevantes para la seguridad de la información tienen ciclos de vida dentro de los cuales son concebidos, especificados, diseñados, desarrollados, probados, implementados, utilizados, mantenidos y eventualmente retirados del servicio y se eliminan. La seguridad de la información debería considerarse en cada etapa. Los nuevos proyectos de desarrollo de sistemas y los cambios en los sistemas existentes proporcionan oportunidades para mejorar los controles de seguridad cuando tomamos en cuenta los riesgos de la organización y las lecciones aprendidas de los incidentes.

0.7 Estándares internacionales relacionados

Si bien este documento ofrece orientación sobre un amplio rango de controles de seguridad de la información que son comúnmente aplicados en muchas organizaciones diferentes, otros documentos de la familia ISO/IEC 27000 proporcionan recomendaciones complementarias o requisitos sobre otros aspectos del proceso completo de gestión de la seguridad de la información.

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

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

---oooOooo---

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

1 Objeto y campo de aplicación

Esta Norma Técnica Peruana proporciona un conjunto de controles de seguridad de la información genéricos de referencia, incluyendo una guía de implementación. Esta Norma Técnica Peruana está diseñada para ser utilizada por organizaciones:

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

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

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

2 Referencias normativas

No hay referencias normativas en esta Norma Técnica Peruana.

3 Términos, definiciones y términos abreviados

3.1 Términos y definiciones

Para los propósitos de esta Norma Técnica Peruana, se aplican los siguientes términos y definiciones.

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

- Plataforma de navegación en línea ISO: disponible en https://www.iso.org/obp
- IEC Electropedia: disponible en https://www.electropedia.org/

3.1.1
control de acceso
medios para garantizar que el acceso físico y lógico a los *activos* (3.1.2) esté autorizado y restringido basado en el negocio y los requisitos de seguridad de la información

3.1.2
activo
cualquier cosa que tenga valor para la organización

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

- los activos primarios:
  - información;
  - procesos de negocio (3.1.27) y actividades;
- los activos de soporte (de los que dependen los activos primarios) de todo tipo, por ejemplo:
  - hardware;
  - software;
  - red;
  - personal (3.1.20);
  - sitio;
  - estructura de la organización.

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

3.1.4
autenticación
provisión de aseguramiento que una característica declarada de una *entidad* (3.1.11) es correcta

3.1.5
autenticidad
propiedad de que una *entidad* (3.1.11) es la que declara ser

3.1.6
cadena de custodia
posesión, movimiento, manipulación y localización demostrables de material desde un punto en el tiempo hasta otro

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

[FUENTE: ISO/IEC 27050-1:2019, 3.1, modificado - Se agregó la "Nota 1 a la entrada"]

3.1.7
información confidencial
información no destinada a estar disponible o divulgada a individuos, *entidades* (3.1.11) o *procesos* (3.1.27) no autorizados

3.1.8
control
medida que mantiene y/o modifica el riesgo

Nota 1 a la entrada: Los controles incluyen, pero no se limitan a, cualquier proceso (3.1.27), política (3.1.24), dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen el riesgo.

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

[FUENTE: ISO 31000:2018, 3.8]

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

[FUENTE: ISO 22301:2019, 3.10]

3.1.10
dispositivo de punto final (endpoint device)
dispositivo de hardware de Tecnología de información y comunicaciones (TIC) conectado a la red

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

3.1.11
entidad
elemento relevante para el propósito de operación de un dominio que tiene una existencia distintiva reconocible

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

EJEMPLO: Una persona, una organización, un dispositivo, un grupo de dichos elementos, un suscriptor 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, servicio o infraestructura de procesamiento de información, o la ubicación física que lo alberga

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

3.1.13
brecha de seguridad de la información
compromiso de la seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados de la información protegida que es transmitida, almacenada o procesada de otro modo

3.1.14
evento de seguridad de la información
ocurrencia que indica una posible *brecha de seguridad de la información* (3.1.13) o falla de los *controles* (3.1.8)

[FUENTE: ISO/IEC 27035-1:2016, 3.3, modificado - "brecha de la seguridad de la información" ha sido reemplazada por "brecha de seguridad de la información"]

3.1.15
incidente de seguridad de la información
uno o múltiples *eventos* (3.1.14) de seguridad de la información relacionados e identificados que pueden dañar los *activos* (3.1.2) de una organización 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 el manejo de *incidentes de seguridad de la información* (3.1.15)

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

3.1.17
sistema de información
conjunto de aplicaciones, servicios, *activos* (3.1.2) de tecnología de la información, u otros componentes de manejo de información

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

3.1.18
parte interesada
stakeholder
persona u organización que puede afectar, verse afectada o percibirse así mismo como afectado 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 pedidos y las *entidades* (3.1.11) que lo originan

3.1.20
personal
personas que trabajan bajo la dirección de la organización

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

3.1.21
información de identificación personal
IIP
cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona natural a la que se relaciona dicha información, o (b) sea o pueda ser directa o indirectamente vinculada a una persona natural

Nota 1 a la entrada: La "persona natural" en la definición es el titular de IIP (3.1.22). Para determinar si un titular de IIP es identificable, se deberían tener en cuenta todos los medios que puedan ser razonablemente utilizados por la parte interesada en privacidad que posee los datos, o por cualquier otra parte, para establecer el vínculo entre el conjunto de IIP y la persona natural.

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

3.1.22
titular de IIP
persona física a la que se relaciona la *información de identificación personal (IIP)* (3.1.21)

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

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

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

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

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

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

3.1.25
evaluación de impacto en la privacidad
PIA
proceso (3.1.27) general para identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de los posibles impactos a la privacidad con respecto al procesamiento de *información de identificación personal (IIP)* (3.1.21), situado dentro de un más amplio marco de referencia en gestión de riesgos de la organización

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

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

[FUENTE: ISO 30000:2009, 3.12]

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

[FUENTE: ISO 9000:2015, 3.4.1, modificada — Se eliminaron las notas a la entrada].

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

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

[FUENTE: ISO 15489-1:2016, 3.14, modificada - Se agregó la “Nota 1 a la entrada”.]

3.1.29
punto de recuperación objetivo
RPO
punto en el tiempo al que la data será recuperada después de que se haya producido una *disrupción* (3.1.9)

[FUENTE: ISO/IEC 27031:2011, 3.12, modificado – "tener que" reemplazado por "será".]

3.1.30
tiempo de recuperación objetivo
RTO
período de tiempo dentro del cual los niveles mínimos de servicios y/o productos y los sistemas de soporte, aplicaciones o funciones serán recuperados después de que haya ocurrido una *disrupción* (3.1.9)

[FUENTE: ISO/IEC 27031:2011, 3.13, modificado – "tener que" reemplazado por "será".]

3.1.31
fiabilidad
propiedad de un comportamiento y resultados previstos consistentes

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

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

3.1.33
información sensible
información que necesita ser protegida de la indisponibilidad, acceso no autorizado, modificación o divulgación pública debido a potenciales efectos adversos en un individuo, organización, seguridad nacional o salubridad pública

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

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

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

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

Nota 2 a la entrada: Algunas organizaciones utilizan otros términos para estas políticas de tema específico.

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

EJEMPLO: Política de tema específico sobre control de acceso (3.1.1), política de tema específico sobre escritorio y pantalla limpios.

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

EJEMPLO: Personal (3.1.20), clientes, suministradores.

3.1.37
dispositivo de punto final de usuario (user endpoint device)
dispositivo de punto final (3.1.10) utilizado por los usuarios para acceder a los servicios de procesamiento de información

Nota 1 a la entrada: El dispositivo de punto final del usuario puede referirse a computadoras de escritorio, laptops, teléfonos inteligentes, tablets, clientes ligeros, entre otros.

3.1.38
vulnerabilidad
debilidad de un *activo* (3.1.2) o *control* (3.1.8) que puede ser explotado por una o más *amenazas* (3.1.34)

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

3.2 Términos abreviados

CABA	control de acceso basado en atributos
LCA	lista de control de accesos
AIN	análisis del impacto en el negocio
TTPD	trae tu propio dispositivo
CAPTCHA	prueba de Turing pública y totalmente automatizada para distinguir entre ordenadores y humanos
CPU	unidad central de procesamiento
CAD	control de acceso discrecional
DNS	sistema de nombres de dominio
GPS	sistema de posicionamiento global
GIA	gestión de identidades y accesos
TIC	tecnología de la 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 la información
SGSI	sistema de gestión de seguridad de la información
MAC	control de acceso obligatorio
PTR	protocolo de tiempo de red
EIP	evaluación de impacto sobre privacidad
IIP	información de identificación personal
PIN	número de identificación personal
PKI	infraestructura de clave pública
PTP	protocolo de tiempo de precisión
RBAC	control de acceso basado en roles
RPO	punto de recuperación objetivo
RTO	tiempo de recuperación objetivo
SAST	prueba de seguridad de aplicación estática
SD	seguro digital
SDN	red definida por software
SD-WAN	red de área extensa definida por software
SIEM	gestión de evento e información de seguridad
SMS	servicio de mensajes cortos
SQL	lenguaje de consulta estructurado
SSO	inicio de sesión única
SWID	identificación de software
UEBA	análisis del comportamiento de usuarios y entidades

UPS	suministro de energía ininterrumpido
URL	localizador uniforme de recursos
USB	bus serial universal
VM	máquina virtual
VPN	red privada virtual
WiFi	wireless fidelity

4 Estructura de este documento

4.1 Capítulos

Este documento está estructurado como sigue:

a) Controles organizacionales (capítulo 5).

b) Controles de personas (capítulo 6).

c) Controles físicos (capítulo 7).

d) Controles tecnológicos (capítulo 8).

Tiene 2 anexos informativos:

- Anexo A - Utilizando atributos
- Anexo B - Correspondencia con ISO/IEC 27002:2013

El Anexo A explica cómo una organización puede utilizar los atributos (véase 4.2) para crear sus propias vistas basadas en los atributos del control definidos en este documento o de su propia creación.

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

4.2 Temas y atributos

La categorización de los controles proporcionados en los capítulos 5 a 8 son referidos como temas.

Los controles están categorizados como:

a) personas, si se refieren a personas individuales;

b) físicos, si se refieren a objetos físicos;

c) tecnológicos, si se refieren a tecnología;

d) de lo contrario, se clasifican como organizacionales.

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

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

a) Tipo de control

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

b) Propiedades de seguridad de la información

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

c) Conceptos de ciberseguridad

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

d) Capacidades operacionales

Las capacidades operativas es un atributo para ver los controles desde la perspectiva profesional de las capacidades de seguridad de la información. Los valores del atributo consisten en Gobernanza, Gestión_de_activos, Protección_de_la_información, Seguridad_de_los_recursos humanos, Seguridad_física, Seguridad_de_sistemas_y_red, Seguridad_de_aplicaciones, Configuración_segura, Gestión_de_identidades_y_accesos, Gestión_de_amenazas_y_vulnerabilidades, Continuidad, Seguridad_de_las_relaciones_con_proveedores, Legal_y_cumplimiento, gestión_de_eventos_de_seguridad_de_la_información y garantizar_la_seguridad_de_la_información.

e) Dominios de seguridad

Dominios de seguridad es un atributo para ver los controles desde la perspectiva de cuatro dominios de seguridad de la información: “Gobernanza y ecosistema” incluye “Gobernanza de la seguridad en sistemas de información y gestión del riesgo” y “Gestión del ecosistema de ciberseguridad” (incluyendo partes interesadas internas y externas); “Protección” incluye “Arquitectura segura de T.I.”, “Administración de seguridad T.I.”, Gestión de identidades y accesos”, “Mantenimiento de la seguridad T.I.” y “seguridad física y del entorno”; “Defensa” incluye “Detección” y “Gestión de incidentes de seguridad en computadoras”; “Resiliencia” incluye “Continuidad de operaciones” y “Gestión de crisis”. Los valores del atributo consisten en Gobernanza_y_Ecosistema, Protección, Defensa y Resiliencia.

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

4.3 Estructura del control

La estructura para cada control contiene lo siguiente:

- **Título del control:** Nombre corto del control
- **Tabla de atributos:** Una tabla que muestra el/los valor(es) de cada atributo para el control dado;
- **Control:** Qué es el control;
- **Finalidad:** Por qué debería implementarse el control;
- **Orientación:** Cómo se debería implementar el control;
- **Otra información:** Texto explicativo o referencias a otros documentos relacionados.

Los subtítulos son utilizados en el texto de orientación para algunos controles a fin de facilitar la legibilidad cuando la orientación es extensa y aborda varios temas. Dichos títulos no se utilizan necesariamente en todo el texto de orientación. Los subtítulos están subrayados.

5 Controles organizacionales

5.1 Políticas para la Seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_y_Eco-sistema #Resilencia

Control

Una política de Seguridad de la información y políticas de tópico específico deberían ser definidas, aprobadas por la gerencia, publicadas, comunicadas y conocidas tanto por el personal como por las partes interesadas relevantes, además revisadas en intervalos planificados y cuando ocurran cambios significativos.

Propósito

Garantizar la idoneidad, adecuación y eficacia continuas en la dirección de la gerencia y el apoyo a la seguridad de la información de acuerdo con los requisitos del negocio, legales, estatutarios, regulatorios y contractuales.

Guía

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

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

a) estrategia y requisitos del negocio;

b) regulación, legislación y contratos;

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

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

a) definición de seguridad de la información;

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

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

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

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

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

g) procedimientos para el manejo de excepciones y excepciones.

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

A menor nivel, la política de seguridad de la información debería estar respaldada por políticas de tópico específico según sea necesario, mayor exigencia en la implementación de controles de seguridad de la información. Las políticas de tópico específico son típicamente estructuradas para abordar las necesidades de ciertos grupos objetivo dentro de una organización o para cubrir ciertas áreas de seguridad. Las políticas de tópico específico deberían estar alineadas con, y complementar a, la política de seguridad de la información de la organización.

Ejemplos de tópicos incluyen:

a) control de acceso;

b) seguridad física y ambiental;

c) gestión de activos;

d) transferencia de información;

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

f) seguridad de redes;

g) gestión de incidentes de seguridad de la información;

h) copias de respaldo;

i) criptografía y gestión de claves;

j) clasificación y manejo de la información;

k) gestión de vulnerabilidades técnicas;

l) desarrollo seguro.

La responsabilidad por el desarrollo, revisión y aprobación de políticas de tópico específico debería asignarse al personal relevante basado en su nivel apropiado de autoridad y competencia técnica. La revisión debería incluir una evaluación de oportunidades de mejora para la política de seguridad de la información de la organización, las políticas de tópico específico y la gestión de seguridad de la información en respuesta a los cambios en:

a) la estrategia de negocios de la organización;

b) el entorno técnico de la organización;

c) regulaciones, estatutos, legislación y contratos;

d) riesgos de seguridad de la información;

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

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

La revisión de la política de seguridad de la información y las políticas de tópico específico deberían tomar en cuenta los resultados de las revisiones por la alta dirección y las auditorías. Se debería considerar la revisión y actualización de otras políticas relacionadas cuando se cambia una política para mantener la coherencia.

La política de seguridad de la información y las políticas de tópico específico deberían ser comunicadas al personal relevante y a las partes interesadas en una forma que sea relevante, accesible y comprensible para el lector previsto. Se debería exigir a los destinatarios de las políticas que conozcan, entiendan y aceptan cumplir con las políticas cuando sea aplicable. La organización puede determinar los formatos y nombres de estos documentos de política que satisfagan las necesidades de la organización. En algunas organizaciones, la política de seguridad de la información y las políticas de tópico específico pueden estar en un solo documento. La organización puede denominar a estas políticas de tópico específico como estándares, directivas, políticas u otros.

Si la política de seguridad de la información o cualquier política de tópico específico es distribuida fuera de la organización, se debería tener cuidado de no revelar información confidencial de manera inapropiada.

La Tabla 1 ilustra las diferencias entre la política de seguridad de la información y una política de tópico específico.

Tabla 1 – Diferencias entre la política de seguridad de la información y una política de tópico específico

	Política de seguridad de la información	**Política de tópico específicos**
Nivel de detalle	General o alto nivel	Especifico y detallado
Documentado y formalmente aprobado por	Alta dirección	Nivel de gestión adecuado

Otra información

Las políticas de tópico específico pueden variar a través de las organizaciones.

5.2 Roles y responsabilidades en seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_y_Eco-sistema #Protección #Resilencia

Control

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

Propósito

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

Guía

La asignación de roles y responsabilidades en seguridad de la información debería realizarse de acuerdo con la política de seguridad de la información y las políticas de tópico específico (véase 5.1). La organización debería definir y gestionar las responsabilidades para:

a) protección de la información y otros activos asociados;

b) realizar procesos específicos de seguridad de la información;

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

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

Estas responsabilidades deberían ser complementadas, cuando sea necesario, con una guía más detallada para sitios e instalaciones de procesamiento de información específicos. Las personas con responsabilidades de seguridad de la información asignadas pueden asignar tareas de seguridad a otros. Sin embargo, siguen siendo responsables de rendir cuentas y deberían determinar que cualquier tarea delegada se haya realizado correctamente.

Cada área de seguridad de la cual los individuos son responsables debería ser definida, documentada y comunicada. Los niveles de autorización deberían definirse y documentarse. Las personas que asumen un rol específico de seguridad de la información deberían ser competentes en conocimiento y habilidades requeridas por el rol y deberían recibir apoyo para mantenerse al día con los desarrollos relacionados con el rol y se les exige cumplir con las responsabilidades del rol.

Otra información

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

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

Dependiendo del tamaño y los recursos de una organización, la seguridad de la información puede estar cubierta por roles dedicados o funciones llevados a cabo en adición a los roles existentes.

5.3 Segregación de funciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernanza #Identidad_y_gestión_de_accesos	#Gobernanza_y_Eco-sistema

Control

Funciones en conflicto y áreas en conflicto deberían ser segregadas.

Propósito

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

Guía

La segregación de funciones y áreas de responsabilidad tiene como objetivo separar las funciones conflictivas entre diferentes individuos para prevenir que un individuo ejecute por sí mismo funciones potencialmente conflictivas.

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

a) iniciar, aprobar y ejecutar un cambio;

b) solicitar, aprobar e implementar derechos de acceso;

c) diseñar, implementar y revisar el código fuente;

d) desarrollar software y administrar sistemas en producción;

e) usar y administrar aplicaciones;

f) utilizar aplicaciones y administrar bases de datos;

g) diseñar, auditar y asegurar los 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 debería aplicarse en la medida de lo posible y practicable. Siempre que sea difícil segregar, se deberían considerar otros controles, como el seguimiento de las actividades, las pistas de auditoría y la supervisión de la gestión.

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

Otra información

No hay otra información.

5.4 Responsabilidad de la gerencia

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_y_Eco-sistema

Control

La gerencia debería requerir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas de tópico específico y los procedimientos de la organización.

Propósito

Asegurar que la gerencia entiende su rol en la seguridad de la información y emprende acciones destinadas a asegurar que todo el personal conozca y cumpla con sus responsabilidades de seguridad de la información.

Guía

La gerencia debería demostrar su apoyo a la política de seguridad de la información, las políticas de tópico específico, los procedimientos y controles de seguridad de la información.

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

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

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

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

d) lograr un nivel de conciencia en seguridad de la información relevante para sus roles y responsabilidades dentro de la organización (véase 6.3);

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

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

g) cuando sea practicable, proporcionar un canal confidencial para reportar violaciones a la política de seguridad de la información, políticas de tópico específico o procedimientos para la seguridad de la información ("denuncia"). Esto puede permitir reportes anónimos, o tener disposiciones para garantizar que el conocimiento de la identidad del reportante sea conocido solo por aquellos que necesitan tratar con dichos reportes;

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

Otra información

No hay otra información.

5.5 Contacto con autoridades

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resilencia

Control

La organización debería establecer y mantener contacto con las autoridades relevantes.

Propósito

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

Guía

La organización debería especificar cuándo y por quién se debería contactar a las autoridades (por ejemplo, fuerzas del orden, organismos reguladores, autoridades de supervisión) y cómo se deberían reportar oportunamente los incidentes de seguridad de la información identificados.

El contacto con las autoridades también deberían utilizarse para facilitar el entendimiento de las expectativas actuales y futuras de estas autoridades (por ejemplo, las regulaciones en seguridad de la información aplicables).

Otra información

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

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

5.6 Contacto con grupos especiales de interés

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa

Control

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

Propósito

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

Guía

La membresía a grupos o foros especiales de interés deberían considerarse como un medio para:

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

b) asegurarse que el entendimiento del entorno de seguridad de la información esté actualizado;

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

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

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

f) proporcionar puntos de enlace adecuados cuando se trate de incidentes de seguridad de la información (véase 5.24 a 5.28).

Otra información

No hay otra información.

5.7 Inteligencia de amenazas

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Gestión_de_amenazas_y_vulnerabilidades	#Defensa #Resilencia

Control

La información relacionada con las amenazas a la seguridad de la información debería ser recopilada y analizada para producir inteligencia sobre las amenazas.

Propósito

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

Guía

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

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

b) reducir el impacto de estas amenazas.

La inteligencia de amenazas se puede dividir en tres capas, todas las cuales deberían considerar:

a) inteligencia estratégica de 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 de amenazas: información sobre metodologías, herramientas y tecnologías del atacante involucrado;

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

La inteligencia de amenazas debería ser:

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

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

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

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

Las actividades de inteligencia de amenazas deberían incluir:

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

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

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

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

e) analizar la información para comprender cómo está relacionada y es significativa para la organización;

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

La inteligencia de amenazas debería analizarse y utilizarse posteriormente:

a) para implementar procesos que incluyan la información obtenida de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la organización;

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

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

Las organizaciones deberían compartir la inteligencia sobre amenazas con otras organizaciones de forma mutua para mejorar la inteligencia sobre amenazas en general.

Otra información

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

La inteligencia de amenazas a menudo es proporcionada por proveedores o asesores independientes, agencias gubernamentales o grupos colaborativos de inteligencia de amenazas.

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

5.8 Seguridad de la información en la gestión de proyectos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Governanza	#Governanza y Ecosystema #Protección

Control

La seguridad de la información debería estar integrada en la gestión de proyectos.

Propósito

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

Guía

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

La gestión de proyectos en uso debería requerir que:

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

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

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

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

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

Las responsabilidades y autoridad para la seguridad de la información relevantes para el proyecto deberían ser definidos y asignados a roles específicos.

Los requisitos de seguridad de la información para los productos o servicios que entregará el proyecto deberían determinarse utilizando varios métodos, incluyendo la derivación de los requisitos de cumplimiento de la política de seguridad de la información, las políticas de tópico específico y regulaciones. 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 operacional.

Los requisitos de seguridad de la información deberían determinarse 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) qué información está involucrada (determinación de la información), cuál es su valor de seguridad correspondiente (clasificación; véase 5.12) y el potencial impacto negativo en el negocio que puede resultar de la falta de seguridad adecuada;

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

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

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

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

f) requisitos derivados de los procesos del negocio, tales como registro y seguimiento de transacciones, requisitos de no repudio;

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

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

i) el nivel de confianza o aseguramiento requerido para que terceros cumplan con la política de seguridad de la información de la organización y las políticas de tópico específico, incluyendo las cláusulas de seguridad relevantes en cualquier acuerdo o contrato.

Otra información

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

ISO/IEC 27005 proporciona orientación sobre el uso de procesos de gestión de riesgos para identificar controles que permitan cumplir con los 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 operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión_de_Activos	#Gobernanza_y_Eco-sistema #Protección

Control

Un inventario de información y otros activos asociados, incluidos los propietarios, debería ser desarrollado y mantenido

Propósito

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

Guía

Inventario

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

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

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

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

La ubicación de un activo debería incluirse en el inventario según sea apropiado.

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

Cada activo debería clasificarse de acuerdo con la clasificación de la información (véase 5.12) asociada a ese activo.

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

Propiedad

Para la información identificada y otros activos asociados, la propiedad del activo debería asignarse a un individuo o grupo y debería identificarse la clasificación (véase 5.12, 5.13). Debería implementarse un proceso para garantizar la asignación oportuna de la propiedad de los activos. La propiedad debería asignarse cuando se crean los activos o cuando se transfieren los activos a la organización. La propiedad de los activos debería reasignarse según sea necesario cuando los propietarios actuales de los activos se van o cambian roles de trabajo.

Deberes del propietario

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

a) se inventarían la información y otros activos asociados;

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

c) la clasificación es revisada periódicamente;

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

e) los requisitos para el uso aceptable de la información y otros activos asociados (véase 5.10) son establecidos;

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

g) la información y otros activos asociados, cuando se eliminan o se ponen a disposición, son manipulados de manera Segura y removidos del inventario;

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

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

Otra información

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

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

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

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

5.10 Uso aceptable de la información y otros activos asociados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_Información	#Gobernanza_y_Ecosistema #Protección

Control

Reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debería ser identificada, documentada e implementada.

Propósito

Para asegurar que la información y otros activos asociados son apropiadamente protegidos, utilizados y manejados.

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. Ellos deberían ser responsables por el uso que hagan de cualquier instalación de procesamiento de información.

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

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

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

c) las actividades de seguimiento que realiza la organización.

Se deberían elaborar procedimientos de uso aceptable para todo el ciclo de vida de la información de acuerdo con su clasificación (véase 5.12) y riesgos determinados. Se deberían considerar los siguientes elementos:

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

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

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

d) almacenamiento de activos asociados con la información de acuerdo con las especificaciones de los fabricantes (véase 7.8);

e) marcado claro de todas las copias de los medios de almacenamiento (electrónicos o físicos) para la atención del destinatario autorizado (véase 7.10);

f) autorización de disposición de información y otros activos asociados y método(s) de borrado soportados (véase 8.10).

Otra información

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

5.11 Retorno de Activos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos	#Protección

Control

El personal y otras partes interesadas, según sea apropiado, deberían devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.

Propósito

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

Guía

El proceso de cambio o terminación debería formalizarse para incluir la devolución de todos los activos físicos y electrónicos entregado previamente que sean propiedad de la organización o confiados a esta.

En los casos en que el personal y otras partes interesadas compren el equipo de la organización o usen su propio equipo personal, se deberían seguir los procedimientos para asegurar que toda la información relevante sea rastreada, transferida a la organización y eliminada de manera segura del equipo (véase 7.14).

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

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

La organización debería identificar y documentar claramente toda la información y otros activos asociados para ser devuelto que puede incluir:

a) dispositivos de punto final de usuario;

b) dispositivos portátiles de almacenamiento;

c) equipo especializado;

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

e) copias físicas de la información.

Otra información

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

5.12 Clasificación de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Protección_de_Información	#Protección #Defensa

Control

La información debería ser clasificada de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos de las partes interesadas relevantes.

Propósito

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

Guía

La organización debería establecer una política de tópico específico sobre la clasificación de la información y comunicarla a todas las partes interesadas relevantes.

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

Las clasificaciones y los controles de protección asociados para la información deberían tener en cuenta las necesidades del negocio para compartir o restringir la información, proteger la integridad de la información y asegurar su disponibilidad, así como los requisitos legales relacionados con la confidencialidad, integridad o disponibilidad de la información. Los activos distintos de la información también pueden clasificarse de conformidad con la clasificación de la información, que es almacenada o procesada por el activo, o de otro modo manejada o protegida por dicho activo.

Los propietarios de la información deberían ser responsables de rendir cuentas por su clasificación.

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

El esquema debería estar alineado con la política de tópico específico sobre el control de acceso (véase 5.1) y debería poder abordar las necesidades del negocio específicas de la organización.

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

El esquema debería ser consistente a través de toda la organización e incluirse en sus procedimientos para que todos clasifiquen la información y otros activos asociados aplicables de la misma manera. De esta manera todos tendrán un entendimiento común de los requisitos de protección y aplicarán una protección adecuada.

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

Otra información

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

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

Un ejemplo de un esquema de clasificación de la confidencialidad de la información se puede basar en cuatro niveles como sigue:

a) la divulgación no causa daño;

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

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

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

5.13 Etiquetado de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Protección_de_la_Información	#Defensa #Protección

Control

Un conjunto de procedimientos apropiado para el etiquetado de información debería ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.

Propósito

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

Guía

Los procedimientos para el etiquetado de la información deberían cubrir la información y otros activos asociados en todos los formatos. El etiquetado debería reflejar el esquema de clasificación establecido en 5.12. Las etiquetas deberían ser fácilmente reconocibles. Los procedimientos deberían brindar orientación sobre dónde y cómo se colocan las etiquetas teniendo en cuenta cómo se accede a la información o cómo se manejan los activos según los tipos de medios de almacenamiento. Los procedimientos pueden definir:

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

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

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

Los ejemplos de técnicas de etiquetado incluyen:

a) etiquetas físicas;

b) encabezados y pies de página;

c) metadatos;

d) marca de agua;

e) sellos de goma.

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

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

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

El personal y otras partes interesadas deberían conocer los procedimientos de etiquetado. Todo el personal debería recibir la capacitación necesaria para asegurar que la información se etiquete correctamente y se manipule de acuerdo a ello.

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

Otra información

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

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

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

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

5.14 Transferencia de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #protección_de_información	#Protección

Control

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

Propósito

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

Guía

Generalidades

La organización debería establecer y comunicar una política de tópico específico sobre la transferencia de información a todas las partes interesadas relevantes. Las reglas, procedimientos y acuerdos para proteger la información en tránsito deberían reflejar la clasificación de la información involucrada. Cuando la información es transferida entre la organización y terceros, se deberían establecer y mantener acuerdos de transferencia (incluida la autenticación del recipiente) para proteger la información en todas las formas en tránsito (véase 5.10).

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

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

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

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

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

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

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

f) confiabilidad y disponibilidad del servicio de transferencia;

g) la política de tópico específico o lineamientos sobre el uso aceptable de las instalaciones de transferencia de información (véase 5.10);

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

NOTA: Pueden existir leyes y regulaciones locales con respecto a la retención y eliminación de registros del negocio.

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

Transferencia electrónica

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

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

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

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

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

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

f) restricciones asociadas con las instalaciones de comunicación electrónica (por ejemplo, prevención de reenvío automático de correo electrónico a direcciones de correo externas);

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

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

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

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

Transferencia de medios de almacenamiento físico

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

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

b) asegurar la dirección correcta y transporte del mensaje;

c) embalaje que proteja el contenido de cualquier daño físico que pueda surgir durante el tránsito y de acuerdo con las especificaciones del fabricante, por ejemplo, protegiendo contra cualquier factor ambiental que pueda reducir la eficacia de la restauración de los medios de almacenamiento, como la exposición al calor, la humedad o los campos electromagnéticos; utilizar estándares técnicos mínimos para el embalaje y la transmisión (por ejemplo, el uso de sobres opacos);

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

e) estándares de identificación del mensajero(courier);

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

g) procedimientos para verificar la identificación de los mensajeros (couriers);

h) una lista aprobada de terceros que proveen servicios de transporte o mensajería dependiendo de la clasificación de la información;

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

Transferencia verbal

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

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

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

c) ser seleccionado en el nivel apropiado para escuchar la conversación;

d) asegurarse de que se implementen los controles de sala apropiados (Por ejemplo, insonorización, puerta cerrada);

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

Otra información

Ninguna otra información.

5.15 Control de Acceso

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestion_de_identidades_y_accesos	#Protección

Control

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

Propósito

Para asegurar el acceso autorizado y prevenir el acceso no autorizado a la información y otros activos asociados.

Guía

Los propietarios de la información y otros activos asociados deberían determinar los requisitos de seguridad de la información y del negocio relacionados con el control de acceso. Debería definirse una política de tópico específico sobre control de acceso que tenga en cuenta estos requisitos y debería comunicarse a todas las partes interesadas relevantes.

Estos requisitos y la política de tópico específico deberían considerar lo siguiente:

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

b) seguridad de las aplicaciones (véase 8.26);

c) acceso físico, que necesita estar respaldado por controles de entrada físicos adecuados (véanse 7.2, 7.3, 7.4);

d) difusión y autorización de la información (por ejemplo, el principio de la necesidad de saber) y los niveles de seguridad y clasificación de la información (véase 5.10, 5.12, 5.13);

e) restricciones para el acceso privilegiado (véase 8.2);

f) segregación de funciones (véase 5.3);

g) la legislación, la regulación y las obligaciones contractuales con respecto a la limitación del acceso a datos o servicios (véase 5.31, 5.32, 5.33, 5.34, 8.3);

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

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

j) la gestión de los derechos de acceso (véase 5.18);

k) registro (véase 8.15).

Las reglas de control de acceso deberían implementarse definiendo y mapeando los derechos y restricciones de acceso apropiados para las entidades relevantes (véase 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 del control de acceso, se pueden asignar roles específicos a grupos de entidades.

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

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

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

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

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

Otra información

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

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

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

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

a) establecer reglas basadas en la premisa del mínimo 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 (véase 5.13) que son iniciados automáticamente por las instalaciones de procesamiento de información y aquellos iniciados a discreción de un usuario;

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

d) cuándo definir y revisar regularmente la aprobación.

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

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

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

5.16 Gestión de identidades

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestion_de_identidades_y_accesos	#Protección

Control

El ciclo de vida completo de identidades debería gestionarse.

Propósito

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

Guía

Los procesos utilizados en el contexto de la gestión de identidades deberían asegurar que:

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

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

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

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

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

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

Las organizaciones deberían contar con un proceso de apoyo para manejar los cambios en la información relacionada con identidades de usuario. Estos procesos pueden incluir la re-verificación de documentos confiables relacionados con la persona.

Al utilizar identidades proporcionadas o emitidas por terceros (por ejemplo, credenciales de redes sociales), la organización debería asegurarse de que las identidades de terceros brinden el nivel de confianza requerido y que los riesgos asociados son conocidos y tratados de forma suficiente. Esto puede incluir controles relacionados con terceros (véase 5.19), así como controles relacionados con la información de autenticación asociada (véase 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 del negocio para establecer una identidad;

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

c) establecer una identidad;

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

e) otorgar o revocar derechos específicos de acceso a la identidad, en base a la debida autorización o decisiones sobre derechos (véase 5.18).

5.17 Información para autenticación

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestion_de_identidades_y_accesos	#Protección

Control

La asignación y gestión de la información de autenticación debería ser controlada por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

Propósito

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

Guía

Asignación de información de autenticación

El proceso de asignación y gestión debería asegurar que:

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

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

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

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

e) la información de autenticación predeterminada que es predefinida o proporcionada por los vendedores es cambiada inmediatamente después de la instalación del sistema o software;

f) se mantienen registros de los eventos significativos relacionados con la asignación y gestión de la información de autenticación y se garantiza su confidencialidad, y se aprueba el método de mantenimiento de registros (por ejemplo, utilizando una herramienta aprobada para almacenamiento de contraseñas).

Responsabilidades del usuario

Cualquier persona que tenga acceso o use información de autenticación debería ser orientada para asegurar que:

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

b) la información de autenticación afectada o comprometida es cambiada inmediatamente después de la notificación de, o cualquier otra indicación de, un compromiso;

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

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

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

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

   4) las contraseñas tienen una longitud mínima;

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

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

Sistema de gestión de contraseñas

Cuando se utilizan contraseñas como información de autenticación, el sistema de gestión de contraseñas debería:

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

b) hacer cumplir contraseñas fuertes de acuerdo con las recomendaciones de buenas prácticas [véase c) de "Responsabilidades del usuario"];

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

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

e) prevenir la reutilización de contraseñas previas;

f) prevenir el uso de contraseñas de uso común y nombres de usuario comprometidos, combinaciones de contraseñas de sistemas hackeados;

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

h) almacenar y transmitir contraseñas en forma protegida.

El cifrado y el hashing de contraseñas deberían realizarse de acuerdo con las técnicas criptográficas aprobadas para contraseñas (véase 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 claves criptográficas, datos almacenados en tokens de hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación y datos biométricos, como escaneos de iris o huellas dactilares. Se puede encontrar información adicional en la serie ISO/IEC 24760.

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

Algunas aplicaciones requieren que una autoridad independiente asigne contraseñas de usuario. En estos casos, a), c) y d) del "Sistema de gestión de contraseñas" no son aplicables.

5.18 Derechos de Acceso

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestion_de_identidades_y_accesos	#Protección

Control

Los derechos de acceso a la información y otros activos asociados deberían ser aprovisionados, revisados, modificados y removidos en concordancia con la política de tópico específico y las reglas para control de acceso de la organización.

Propósito

Para asegurar que el acceso a la información y otros activos asociados este definida y autorizada de acuerdo con los requisitos del negocio.

Guía

Provisión y revocación de los derechos de acceso

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

a) obtener autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados (véase 5.9). Una aprobación por separado de los derechos de acceso por parte de la gerencia también puede ser apropiada;

b) considerando los requisitos del negocio y la política de tópico específico y las reglas sobre el control de acceso de la organización;

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

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

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

f) verificar que el nivel de acceso otorgado esté de acuerdo con las políticas de tópico específico sobre control de acceso (véase 5.15) y sea consistente con otros requisitos de seguridad de la información, como la segregación de funciones (véase 5.3);

g) asegurar que los derechos de acceso estén activados (por ejemplo, por parte de los proveedores de servicios) solo después de que los procedimientos de autorización se han completado satisfactoriamente;

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

i) modificar los derechos de acceso de los usuarios que han cambiado de roles o trabajos;

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

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

Revisión de los derechos de acceso

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

a) los derechos de acceso de los usuarios después de cualquier cambio dentro de la misma organización (por ejemplo, cambio de trabajo, promoción, descenso) o terminación del empleo (véase 6.1 a 6.5);

b) autorizaciones de derechos de acceso privilegiado.

Consideración antes del cambio o terminación del empleo

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

a) si la terminación o cambio es iniciado por el usuario o por la gerencia y la razón de la terminación;

b) las responsabilidades actuales del usuario;

c) el valor de los activos actualmente accesibles.

Otra información

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

Debería considerarse la posibilidad de incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta acceder sin autorización (véase 5.20, 6.2, 6.4, 6.6).

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

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

5.19 Seguridad de la información en las relaciones con los proveedores

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_las_relaciones_con_proveedores	#Gobernanza_y_Ecosistema #Protección

Control

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

Propósito

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

Guía

La organización debería establecer y comunicar una política de tópico específico sobre las relaciones con los proveedores a todas las partes interesadas relevantes.

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

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

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

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

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

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

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

1) el uso que hacen los proveedores de la información de la organización y otros activos asociados, incluidos los riesgos originados desde el personal potencialmente malicioso del proveedor;

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

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

h) mitigar la no conformidad de un proveedor, ya sea que se haya detectado a través del monitoreo o por otros medios;

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

j) resiliencia y, si es necesario, medidas de recuperación y contingencia para asegurar 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) concienciación y entrenamiento para el personal de la organización que interactúa con el personal del proveedor con respecto a las reglas de compromiso apropiadas, políticas de tópico específico, procesos, procedimientos y comportamiento en función del tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la organización;

l) gestionar la transferencia de información necesaria, otros activos asociados y cualquier otra cosa que necesite ser cambiada y garantizar que la seguridad de la información se mantenga durante todo el período de transferencia;

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

1) desaprovisionamiento de los derechos de acceso;

2) manejo de la información;

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

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

6) gestión de registros;

7) retorno de activos;

8) eliminación segura de información y otros activos asociados;

9) requisitos de confidencialidad en curso;

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

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

Otra información

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

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

b) implementar controles compensatorios según sea necesario con base en la evaluación de riesgo.

La información puede ser puesta en riesgo por proveedores con una gestión de seguridad de la información inadecuada. Deberían determinarse y aplicarse controles para gestionar el acceso del proveedor a la información y otros activos asociados. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de no divulgación o técnicas criptográficas. Otro ejemplo son los riesgos de protección de datos personales cuando el acuerdo con el proveedor involucra la transferencia o el acceso a información a través de las fronteras. La organización necesita ser consciente de que la responsabilidad legal o contractual por proteger la información sigue siendo de la organización.

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

Ver ISO/IEC 27036-2 para más detalles.

5.20 Abordar la seguridad dentro de los acuerdos con proveedores

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_las_relaciones_con_proveedores	#Gobernanza_y_Eco-sistema #Protección

Control

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

Propósito

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

Guía

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

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

a) descripción de la información a proporcionar o acceder y métodos para proporcionar o acceder a la información;

b) clasificación de la información de acuerdo con el esquema de clasificación de la organización (véase 5.10, 5.12, 5.13);

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

d) los requisitos legales, estatutarios, regulatorios y contractuales, incluida la protección de datos, el manejo de la información de identificación personal (IIP), los derechos de propiedad intelectual y los derechos de autor y una descripción de cómo se asegura su cumplimiento;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Las organizaciones deberían establecer y mantener un registro de acuerdos con partes externas (por ejemplo, contratos, memorandos de entendimiento, acuerdos de intercambio de información) para realizar un seguimiento de adónde va su información. Las organizaciones también deberían revisar, validar y actualizar periódicamente sus acuerdos con partes externas para asegurarse de que siguen siendo necesarios y aptos para su propósito con los capítulos de seguridad de la información pertinentes.

Otra información

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

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

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_las_relaciones_con_proveedores	#Gobernanza_y_Eco-sistema #Protección

Control

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

Propósito

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

Guía

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

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

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

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

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

e) solicitar que los proveedores de productos TIC proporcionen información que describa las funciones de seguridad implementadas de sus productos y las configuraciones requeridas para su operación segura;

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

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

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

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

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

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

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

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

Otra información

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

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

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

Las cadenas de suministro de TIC que se abordan aquí incluyen servicios en la nube.

Ejemplos de cadenas de suministro de TIC son:

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

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

c) servicios de hospedaje, donde el proveedor depende de mesas de servicio externas que incluyen primera, segunda y terceros niveles de soporte.

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

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

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_las_relaciones_con_proveedores	#Gobernanza_y_Ecosistema #Protección #Defensa #Aseguramiento_de_la_seguridad_de_la_información

Control

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

Propósito

Para mantener un nivel acordado de seguridad de la información y prestación de servicios en línea con los acuerdos del proveedor.

Guía

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

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

a) monitorear los niveles de rendimiento del servicio para verificar la conformidad con los acuerdos;

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

1) mejoras a los servicios actuales ofrecidos;

2) desarrollo de nuevas aplicaciones y sistemas;

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

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

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

1) cambios y mejoras a las redes;

2) uso de nuevas tecnologías;

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

4) nuevas herramientas y entornos de desarrollo;

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

6) cambio de subproveedores;

7) subcontratación a otro proveedor;

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

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

f) proporcionar información sobre incidentes de seguridad de la información y revisar esta información según lo requieran los acuerdos y cualquier guía y procedimiento de apoyo;

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

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

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

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

k) asegurarse de que el proveedor mantenga una capacidad de servicio suficiente junto con planes viables diseñados para garantizar que se mantengan los niveles de continuidad del servicio acordados después de fallas importantes en el servicio o desastres (véanse 5.29, 5.30, 5.35, 5.36, 8.14);

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

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

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

Otra información

Ver ISO/IEC 27036-3 para más detalles.

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_relaciones_con_proveedores	#Gobernanza_y_Eco-sistema #Protección

Control

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

Propósito

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

Guía

La organización debería establecer y comunicar una política específica de un tema sobre el uso de servicios en la nube para todas las partes interesadas pertinentes.

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

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

La organización debería definir:

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

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

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

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

e) cómo obtener y utilizar las capacidades de seguridad de la información proporcionadas por el proveedor de servicios en la nube; f) cómo obtener garantías sobre los controles de seguridad de la información implementados por los proveedores de servicios en la nube;

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

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

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

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

Los acuerdos de servicios en la nube a menudo están predefinidos y no están abiertos a negociación. Para todos los servicios en la nube, la organización debería revisar los acuerdos de servicios en la nube con los proveedores de servicios en la nube. Un acuerdo de servicio en la nube debería abordar los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la organización, con objetivos de nivel de servicio en la nube y objetivos cualitativos de servicio en la nube apropiados. La organización también debería realizar evaluaciones de riesgos relevantes para identificar los riesgos asociados con el uso del servicio en la nube. Cualquier riesgo residual relacionado con el uso del servicio en la nube debería ser claramente identificado y aceptado por la gerencia adecuada de la organización.

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

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

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

c) implementar soluciones de protección y monitoreo de malware;

d) procesar y almacenar la información confidencial de la organización en ubicaciones aprobadas (por ejemplo: país o región en particular) o dentro o sujeto a una jurisdicción en particular;

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

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

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

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

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

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

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

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

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

c) el uso de proveedores de servicios en la nube similares u otros subcontratistas (incluido el cambio o el uso de nuevos partidos).

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

Otra información

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

Puede encontrar información adicional relacionada con los servicios en la nube en ISO/IEC 17788, ISO/IEC 17789 e ISO/IEC 22123-1. Los detalles relacionados con la portabilidad de la nube en apoyo de las estrategias de salida se pueden encontrar en ISO/IEC 19941. Los detalles relacionados con la seguridad de la información y los servicios de nube pública se describen en ISO/IEC 27017. Se describen los detalles relacionados con la protección de IIP en nubes públicas que actúan como procesador de IIP. en ISO/IEC 27018. Las relaciones con los proveedores de servicios en la nube están cubiertas por ISO/IEC 27036-4 y los acuerdos de servicios en la nube y sus contenidos se tratan en la serie ISO/IEC 19086, con la seguridad y privacidad cubiertas específicamente por ISO/IEC 19086- 4.

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gobernanza #Gestion_de_eventos-_de_seguridad_de_la_información	#Defensa

Control

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

Propósito

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

Guía

Roles y responsabilidades

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

Se debería considerar lo siguiente:

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

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

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

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

e) establecer un proceso para identificar la capacitación, la certificación y los servicios profesionales continuos requeridos desarrollo para el personal de respuesta a incidentes.

Procedimientos de gestión de incidentes

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

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

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

b) monitorear (véase 8.15 y 8.16), detectar (véase 8.16), clasificar (véase 5.25), analizar y reportar (véase 6.8) de eventos e incidentes de seguridad de la información (por medios humanos o automáticos);

c) gestionar los incidentes de seguridad de la información hasta su conclusión, incluida la respuesta y el escalamiento (véase 5.26), según el tipo y la categoría del incidente, la posible activación de la gestión de crisis y la activación de los planes de continuidad, la recuperación controlada de un incidente y la comunicación a las partes interesadas externas;

d) coordinación con partes interesadas internas y externas tales como autoridades, grupos de interés externo y foros, proveedores y clientes (véase 5.5 y 5.6);

e) registrar las actividades de gestión de incidentes;

f) manejo de evidencia digital (véase 5.28);

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

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

Procedimientos de reporte

Los procedimientos de reporte deberían incluir:

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

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

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

d) elaboración de reportes de incidencias.

Cualquier requisito externo sobre el informe de incidentes a las partes interesadas relevantes dentro del marco de tiempo definido (por ejemplo, requisitos de notificación de incumplimiento a los reguladores) debería tenerse en cuenta al implementar los procedimientos de gestión de incidentes.

Otra información

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

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

5.25 Evaluación y decisión sobre eventos de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gestion_de_eventos-_de_seguridad_de_la_información	#Defensa

Control

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

Propósito

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

Guía

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

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

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

Otra información

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

5.26 Respuesta a incidentes de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gestion_de_eventos-_de_seguridad_de_la_información	#Defensa

Control

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

Propósito

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

Guía

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

Los incidentes de seguridad de la información deberían ser respondidos por un equipo designado con la competencia requerida (véase 5.24).

La respuesta debería incluir lo siguiente:

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

b) recolectar evidencia (véase 5.28) tan pronto como sea posible después de la ocurrencia;

c) escalada, según sea necesario, incluidas las actividades de gestión de crisis y posiblemente invocando planes de continuidad del negocio (véase 5.29 y 5.30);

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

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

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

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

h) realizar análisis forenses de seguridad de la información, según se requiera (véase 5.28);

i) realizar un análisis posterior al incidente para identificar la causa raíz. Asegúrese de que esté documentado y comunicado de acuerdo con los procedimientos definidos (véase 5.27);

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

Otra información

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

5.27 Aprendizaje de los incidentes de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #proteger	#Gestion_de_eventos-_de_seguridad_de_la_información	#Defensa

Control

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

Propósito

Para reducir la probabilidad o las consecuencias de futuros incidentes.

Guía

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

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

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

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

c) mejorar la formación de conciencia del usuario (véase 6.3) proporcionando ejemplos de lo que puede suceder, cómo responder a tales incidentes y cómo evitarlos en el futuro.

Otra información

La serie ISO/IEC 27035 proporciona más orientación.

5.28 Recolección de evidencia

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestion_de_eventos-_de_seguridad_de_la_información	#Defensa

Control

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

Propósito

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

Guía

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

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

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

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

c) cualquier sistema de información del que se hayan obtenido pruebas funcionaba correctamente en el momento en que se registró la prueba.

Cuando esté disponible, la certificación u otros medios relevantes de calificación del personal y las herramientas deberían ser buscado, a fin de fortalecer el valor de la prueba conservada.

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

Otra información

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

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

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

5.29 Seguridad de la información durante una disrupción

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Continuidad	#Protección #Resilencia

Control

La organización debería planificar cómo mantener la seguridad de la información en un nivel apropiado durante una disrupción.

Propósito

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

Guía

La organización debería determinar sus requisitos para adaptar los controles de seguridad de la información durante la disrupción. Los requisitos de seguridad de la información deberían incluirse en los procesos de gestión de la continuidad del negocio.

Los planes deberían desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos comerciales críticos luego de una disrupción o falla. La seguridad de la información debería restaurarse al nivel requerido y en los plazos requeridos. La organización debería implementar y mantener:

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

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

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

Otra información

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

La información sobre la gestión de la continuidad del negocio se puede encontrar en ISO 22313 e ISO 22301 y la información sobre el análisis de impacto en el negocio (AIN) se puede encontrar en ISO/TS 22317.

5.30 Preparativos TIC para la continuidad del negocio

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Correctivo	#Disponibilidad	#Responder	#Continuidad	##Resilencia

Control

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

Propósito

Asegurar la disponibilidad de la información de la organización y otros activos asociados durante la ruptura.

Guía

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

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

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

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

La organización debería asegurarse de que:

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

b) Planes de continuidad de las TIC, incluidos los procedimientos de respuesta y recuperación que detallen cómo la organización planifica como gestionar una disrupción del servicio de TIC, son:

1) evaluado regularmente a través de ejercicios y pruebas;

2) aprobado por la gerencia;

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

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

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

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

Otra información

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

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

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

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

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

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

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

5.31 Requisitos legales, estatutarios, regulatorios y contractuales

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_y_legal	#Gobernanza_y_Eco-sistema #Protección

Control

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

Propósito

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

Guía

Generalidades

Los requisitos externos, incluidos los requisitos legales, estatutarios, regulatorios o contractuales, deberían ser teniendo en cuenta cuando:

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

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

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

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

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

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

Legislación y reglamentos

La organización debería:

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

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

— realiza negocios en otros países;

— usa productos y servicios de otros países donde las leyes y reglamentos pueden afectar la organización;

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

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

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

Criptografía

La criptografía es un área que a menudo tiene requisitos legales específicos. Cumplimiento de los correspondientes deberían tenerse en cuenta los acuerdos, leyes y reglamentos relacionados con los siguientes elementos:

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

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

c) restricciones en el uso de criptografía;

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

e) vigencia de firmas digitales, sellos y certificados.

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

Contratos

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

a) contratos con clientes;

b) contratos con proveedores (véase 5.20);

c) contratos de Seguro

Otra información

Ninguna otra información.

5.32 Derechos de propiedad intelectual

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_y_legal	#Gobernanza_y_Eco-sistema

Control

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

Propósito

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

Guía

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

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

b) publicar procedimientos para la conformidad con los derechos de propiedad intelectual que definen el uso conforme de software y productos de información;

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

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

e) mantener prueba y evidencia de propiedad de licencias, manuales, entre otros;

f) asegurarse de que no se exceda el número máximo de usuarios o recursos (por ejemplo, CPUs) permitidos dentro de la licencia;

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

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

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

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

k) no duplicar, convertir a otro formato o extraer de grabaciones comerciales (video, audio) distintas de Lipceenrsmeditttoe:dBbrayvocoLpópyerzig, Nhtatlaalwy Mosr las licencias aplicables;

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

Otra información

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

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

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

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

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

5.33 Protección de registros

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_y_legal #Gestión_de_activos #Protección_de_la_información	#Defensa

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

Control

Los registros deberían protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.

Propósito

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

Guía

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

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

b) elaborar un programa de retención que defina los registros y el período de tiempo durante el cual deberían ser retenidos.

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

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

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

Cuando se elijan medios de almacenamiento electrónico, se deberían establecer procedimientos para garantizar la capacidad de acceder a los registros (tanto los medios de almacenamiento como la legibilidad del formato) durante todo el período de retención para salvaguardar contra pérdidas debido a futuros cambios tecnológicos. Todas las claves criptográficas relacionadas y los programas asociados con archivos cifrados o firmas digitales también deberían conservarse para permitir el descifrado de los registros durante el tiempo que se conservan (véase 8.24).

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

Otra información

Los registros documentan eventos o transacciones individuales o pueden formar agregados que han sido diseñados para documentar procesos de trabajo, actividades o funciones. Ambos son evidencia de actividad comercial y activos de información. Cualquier conjunto de información, independientemente de su estructura o forma, puede gestionarse como un registro. Esto incluye información en forma de documento, una recopilación de datos u otros tipos de información digital o análoga que se crean, capturan y gestionan en el curso del negocio.

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

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

5.34 Privacidad y protección de IIP

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Protección_de_información #Cumplimiento_y_legal	#Protección

Control

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

Propósito

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

Guía

La organización debería establecer y comunicar una política específica sobre el tema de la privacidad y la protección de IIP a todas las partes interesadas relevantes.

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

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

La responsabilidad por el manejo de la IIP debería abordarse teniendo en cuenta la legislación y reglamentos Se deberían implementar medidas técnicas y organizativas apropiadas para proteger la IIP.

Otra información

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

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

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

5.35 Revisión independiente de la seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #proteger	#Aseguramiento_de_la_seguridad_de_la_información	#Gobernanza_y_Ecosistema

Control

El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debería revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

Propósito

Para garantizar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información.

Guía

La organización debería tener procesos para realizar revisiones independientes.

La gerencia debería planificar e iniciar revisiones periódicas independientes. Las revisiones deberían incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad de la información, incluidas las políticas y otros controles.

Dichas revisiones deberían ser realizadas por personas independientes del área bajo revisión (por ejemplo, la función de auditoría interna, un gerente independiente o una organización externa especializada en tales revisiones). Las personas que lleven a cabo estas revisiones deberían tener la competencia adecuada. La persona que realiza las revisiones no debería estar en la línea de autoridad para garantizar que tenga la independencia para realizar una evaluación.

Los resultados de las revisiones independientes deberían informarse a la dirección que inició las revisiones y, si procede, a la alta dirección. Estos registros deberían mantenerse.

Si las revisiones independientes identifican que el enfoque y la implementación de la organización para gestionar la seguridad de la información son inadecuados [p. los objetivos y requisitos documentados no se cumplen o no se ajustan a la dirección para la seguridad de la información establecida en la política de seguridad de la información y las políticas de tópico específico (véase 5.1)], la gerencia debería iniciar acciones correctivas.

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

a) leyes y reglamentos que afectan el cambio de la organización;

b) ocurren incidentes significativos;

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

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

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

Otra información

ISO/IEC 27007 e ISO/IEC TS 27008 brindan orientación para llevar a cabo revisiones independientes.

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_y_legal #Protección_de_informa ción	#Gobernanza_ y_Ecosistema

Control

El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos del tema debería revisarse periódicamente.

Propósito

Para garantizar que la seguridad de la información se implemente y opere de acuerdo con la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos del tema.

Guía

Los gerentes, propietarios de servicios, productos o información deberían identificar cómo revisar que se cumplan los requisitos de seguridad de la información definidos en la política de seguridad de la información, las políticas de tópico específico, las reglas, los estándares y otras reglamentaciones aplicables. Se deberían considerar herramientas automáticas de medición y generación de informes para una revisión periódica eficiente.

Si se encuentra algún incumplimiento como resultado de la revisión, los gerentes deberían:

a) identificar las causas del incumplimiento;

b) evaluar la necesidad de acciones correctivas para lograr el cumplimiento;

c) implementar acciones correctivas apropiadas;

d) revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidades

Los resultados de las revisiones y acciones correctivas llevadas a cabo por los gerentes, propietarios de servicios, productos o información deberían registrarse y estos registros deberían mantenerse. Los gerentes deberían informar los resultados a las personas que realizan revisiones independientes (véase 5.35) cuando se lleva a cabo una revisión independiente en el área de su responsabilidad.

Las acciones correctivas deberían completarse de manera oportuna según corresponda al riesgo. Si no se completa para la próxima revisión programada, el progreso debería al menos abordarse en esa revisión.

Otra información

El monitoreo operativo del uso del sistema está cubierto en 8.15, 8.16, 8.17.

5.37 Procedimientos operativos documentados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión_de_activos #Seguridad_física #Seguridad_de_sistemas_y_redes #Seguridad_de_aplicación #Configuración_segura #Gestión_de_identidad_y_acceso #Gestión_de_amenazas_y_vulnerabilidades #Continuidad #Gestión_de_eventos_de_seguridad_de_la_información	#Gobernanza_y_Ecosistema #Protección #Defensa

Control

Los procedimientos operativos para las instalaciones de procesamiento de información deberían documentarse y ponerse a disposición del personal que los necesite.

Propósito

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

Guía

Deberían prepararse procedimientos documentados para las actividades operativas de la organización asociadas con la seguridad de la información, por ejemplo:

a) cuando la actividad deba ser realizada de la misma manera por muchas personas;

b) cuando la actividad se realiza con poca frecuencia y cuando se realiza la próxima vez es probable que se haya olvidado el procedimiento;

c) cuando la actividad sea nueva y presente un riesgo si no se realiza correctamente;

d) antes del traspaso de la actividad al nuevo personal.

Los procedimientos operativos deberían especificar:

a) la persona responsable;

b) la instalación y configuración segura de sistemas;

c) procesamiento y manejo de información, tanto automatizado como manual;

d) respaldo (véase 8.13) y resiliencia;

e) requisitos de programación, incluidas las interdependencias con otros sistemas;

f) instrucciones para el manejo de errores u otras condiciones excepcionales [p. restricciones en el uso de programas de utilidad (véase 8.18)], que pueden surgir durante la ejecución del trabajo;

g) contactos de soporte y escalamiento, incluidos contactos de soporte externo en caso de dificultades operativas o técnicas inesperadas;

h) instrucciones de manejo de medios de almacenamiento (véase 7.10 y 7.14);

i) procedimientos de reinicio y recuperación del sistema para su uso en caso de falla del sistema;

j) la gestión de la pista de auditoría y la información de registro del sistema (véase 8.15 y 8.17) y el monitoreo de video sistemas (véase 7.4);

k) procedimientos de monitoreo tales como capacidad, desempeño y seguridad (véase 8.6 y 8.16);

l) instrucciones de mantenimiento.

Los procedimientos operativos documentados deberían revisarse y actualizarse cuando sea necesario. Los cambios a los procedimientos operativos documentados deberían ser autorizados. Cuando sea técnicamente factible, los sistemas de información deberían administrarse de manera consistente, utilizando los mismos procedimientos, herramientas y utilidades.

Otra información

Ninguna otra información.

6 Controles de personal

6.1 Selección

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deberían llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y deberían ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos percibidos.

Propósito

Asegurar que todo el personal sea elegible y adecuado para las funciones para las que se le considera y siga siendo elegible y adecuado durante su empleo.

Guía

Se debería realizar un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. Cuando estas personas sean contratadas a través de proveedores de servicios, los requisitos de selección deberían incluirse en los acuerdos contractuales entre la organización y los proveedores.

La información sobre todos los candidatos que se están considerando para puestos dentro de la organización debería recopilarse y manejarse teniendo en cuenta la legislación pertinente existente en la jurisdicción correspondiente. En algunas jurisdicciones, la organización puede estar legalmente obligada a informar a los candidatos de antemano sobre las actividades de selección.

La verificación debería tener en cuenta toda la privacidad relevante, la protección de IIP y la información basada en el empleo, legislación y debería, cuando esté permitido, incluir lo siguiente:

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

b) una verificación (de integridad y precisión) del currículum vitae del solicitante;

c) confirmación de las calificaciones académicas y profesionales reclamadas;

d) verificación de identidad independiente (por ejemplo, pasaporte u otro documento aceptable emitido por las autoridades correspondientes);

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

Cuando se contrata a una persona para una función específica de seguridad de la información, las organizaciones deberían asegurarse de que el candidato:

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

b) se puede confiar para asumir el rol, especialmente si el rol es crítico para la organización.

Cuando un trabajo, ya sea en el nombramiento inicial o en la promoción, implique que la persona tenga acceso a instalaciones de procesamiento de información y, en particular, si esto implica el manejo de información confidencial (por ejemplo, información financiera, información personal o información de atención médica), la organización también debería considerar más, verificaciones más detalladas.

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

En situaciones en las que la verificación no se puede completar de manera oportuna, se deberían implementar controles de mitigación hasta que se haya terminado la revisión, por ejemplo:

a) incorporación retrasada;

b) retraso en el despliegue de los activos corporativos;

c) embarque con acceso reducido;

d) terminación del empleo.

Los controles de verificación deberían repetirse periódicamente para confirmar la idoneidad continua del personal, según la importancia del rol de una persona.

Otra información

No hay otra información.

6.2 Términos y condiciones del empleo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Los acuerdos contractuales de empleo deberían establecer las responsabilidades del personal y de la organización con respecto a la seguridad de la información.

Propósito

Para garantizar que el personal comprenda sus responsabilidades de seguridad de la información para las funciones para las que son considerados.

Guía

Las obligaciones contractuales para el personal deberían tener en cuenta la política de seguridad de la información de la organización y las políticas de tópico específico relevante. Además, se pueden aclarar y señalar los siguientes puntos:

a) acuerdos de confidencialidad o de no divulgación que el personal al que se le da acceso a información confidencial debería firmar antes de que se le dé acceso a la información y otros activos asociados (véase 6.6);

b) responsabilidades y derechos legales [p. en relación con las leyes de derechos de autor o la legislación de protección de datos (véase 5.32 y 5.34)];

c) responsabilidades para la clasificación de la información y la gestión de la información de la organización y otros activos asociados, instalaciones de procesamiento de información y servicios de información manejados por el personal (véase 5.9 a 5.13);

d) responsabilidades por el tratamiento de la información recibida de los interesados;

e) acciones a tomar si el personal ignora los requisitos de seguridad de la organización (véase 6.4).

Las funciones y responsabilidades de seguridad de la información deberían comunicarse a los candidatos durante el proceso previo al empleo.

La organización debería asegurarse de que el personal esté de acuerdo con los términos y condiciones relacionados con la seguridad de la información. Estos términos y condiciones deberían ser apropiados para la naturaleza y el grado de acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información. Los términos y condiciones relacionados con la seguridad de la información deberían revisarse cuando cambien las leyes, los reglamentos, la política de seguridad de la información o las políticas específicas de un tema.

En su caso, las responsabilidades contenidas en los términos y condiciones de empleo deberían continuar durante un período definido después de la finalización del empleo (véase 6.5).

Otra información

Se puede utilizar un código de conducta para establecer las responsabilidades de seguridad de la información del personal con respecto a la confidencialidad, la protección de la IIP, la ética, el uso adecuado de la información de la organización y otros activos asociados, así como las prácticas respetables esperadas por la organización.

Se puede exigir a una parte externa, con la que está asociado el personal del proveedor, que celebre acuerdos contractuales en nombre de la persona contratada.

Si la organización no es una entidad legal y no tiene empleados, el equivalente de contrato acuerdo y los términos y condiciones se pueden considerar en línea con la guía de este control.

6.3 Conciencia, educación y entrenamiento sobre la seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_recursos_humanos	#Gobernanza_y_Ecosistema

Control

El personal de la organización y las partes interesadas relevantes deberían recibir una adecuada concienciación, educación y capacitación en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral.

Propósito

Para garantizar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades de seguridad de la información.

Guía

Generalidades

Se debería establecer un programa de concientización, educación y capacitación en seguridad de la información de acuerdo con la política de seguridad de la información de la organización, las políticas de tópico específico y los procedimientos relevantes sobre seguridad de la información, teniendo en cuenta la información de la organización que debería protegerse y los controles de seguridad de la información que se han implementado. para proteger la información.

La concientización, la educación y la capacitación en seguridad de la información deberían llevarse a cabo periódicamente. La concientización, la educación y la capacitación iniciales pueden aplicarse al personal nuevo y a aquellos que se transfieran a nuevos puestos o roles con requisitos de seguridad de la información sustancialmente diferentes.

La comprensión del personal debería evaluarse al final de una actividad de sensibilización, educación o formación.

Conciencia

Probar la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y formación.

Un programa de concientización sobre la seguridad de la información debería tener como objetivo que el personal sea consciente de sus responsabilidades con respecto a la seguridad de la información y los medios por los cuales se cumplen esas responsabilidades.

El programa de concientización debería planificarse teniendo en cuenta las funciones del personal en la organización, incluido el personal interno y externo (por ejemplo, consultores externos, personal del proveedor). Las actividades del programa de concientización deberían programarse a lo largo del tiempo, preferiblemente con regularidad, para que las actividades se repitan y cubran al personal nuevo. También debería basarse en las lecciones aprendidas de los incidentes de seguridad de la información.

El programa de sensibilización debería incluir una serie de actividades de sensibilización a través de canales físicos o virtuales adecuados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas, sesiones informativas, módulos de aprendizaje y correos electrónicos.

La concientización sobre la seguridad de la información debería cubrir aspectos generales tales como:

a) el compromiso de la dirección con la seguridad de la información en toda la organización;

b) las necesidades de familiaridad y conformidad con respecto a las normas y obligaciones de seguridad de la información aplicables, teniendo en cuenta la política de seguridad de la información y las políticas, estándares, leyes, estatutos, reglamentos, contratos y acuerdos específicos del tema;

c) responsabilidad personal por las propias acciones e inacciones, y responsabilidades generales para asegurar o proteger la información que pertenece a la organización y las partes interesadas;

d) procedimientos básicos de seguridad de la información (como informes de incidentes de seguridad de la información) y controles básicos (como seguridad de contraseñas, controles de malware y escritorios limpios);

e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre asuntos de seguridad de la información, incluidos más materiales de concientización sobre la seguridad de la información.

Educación y entrenamiento

La organización debería identificar, preparar e implementar un plan de entrenamiento adecuado para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y experiencia 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 acciones y adquirirlas.

El programa de educación y entrenamiento debería considerar diferentes formas [p. conferencias o autoestudios, ser asesorado por personal experto o consultores (capacitación en el trabajo), rotar a los miembros del personal para seguir diferentes actividades, reclutar personas ya capacitadas y contratar consultores]. Puede usar diferentes medios de entrega, incluidos el aprendizaje en el aula, a distancia, basado en la web, a su propio ritmo y otros. El personal técnico debería mantener actualizados sus conocimientos suscribiéndose a boletines y revistas o asistiendo a congresos y eventos destinados a la mejora técnica y profesional.

Otra información

Al redactar un programa de concientización, es importante no solo centrarse en el 'qué' y el 'cómo', sino también en el 'por qué', cuando sea posible. Es importante que el personal comprenda el objetivo de la seguridad de la información y el efecto potencial, positivo y negativo, sobre la organización de su propio comportamiento.

La concientización, la educación y el entrenamiento en seguridad de la información pueden ser parte de, o llevarse a cabo en colaboración con otras actividades, por ejemplo, administración general de la información, TIC, seguridad, privacidad o capacitación en seguridad.

6.4 Proceso disciplinario

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #responder	#Seguridad_en_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Se debería formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.

Propósito

Asegurar que el personal y otras partes interesadas relevantes comprendan las consecuencias de la violación de la política de seguridad de la información, para disuadir y tratar adecuadamente al personal que cometió la violación.

Guía

El proceso disciplinario no debería iniciarse sin la verificación previa de que se ha producido una violación de la política de seguridad de la información (véase 5.28).

El proceso disciplinario formal debería prever una respuesta graduada que tenga en cuenta factores tales como:

a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad del incumplimiento y sus consecuencias;

b) si el delito fue intencional (malicioso) o no intencional (accidental);

c) si se trata o no de una primera o reiterada infracción;

d) si el infractor fue debidamente capacitado o no.

La respuesta debería tener en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales y comerciales pertinentes, así como otros factores que sean necesarios. El proceso disciplinario también debería utilizarse como elemento disuasorio para evitar que el personal infrinja la política de seguridad de la información, las políticas y los procedimientos específicos de la seguridad de la información. Las violaciones deliberadas de la política de seguridad de la información pueden requerir acciones inmediatas.

Otra información

Siempre que sea posible, la identidad de las personas sujetas a medidas disciplinarias debería protegerse de conformidad con los requisitos aplicables.

Cuando las personas demuestran un comportamiento excelente con respecto a la seguridad de la información, pueden ser recompensadas para promover la seguridad de la información y fomentar el buen comportamiento.

6.5 Responsabilidades después de la terminación o cambio de empleo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_recursos_humanos #Gestión_de_activos	#Gobernanza_y_Eco-sistema

Control

Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo deberían definirse, aplicarse y comunicarse al personal pertinente y otras partes interesadas.

Propósito

Para proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo o contratos

Guía

El proceso para gestionar la terminación o el cambio de empleo debería definir qué responsabilidades y deberes de seguridad de la información deberían permanecer vigentes después de la terminación o el cambio. Esto puede incluir la confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos, así como las responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (véase 6.6). Las responsabilidades y deberes que sigan vigentes después de la terminación del empleo o contrato deberían estar contenidos en los términos y condiciones de empleo (véase 6.2), contrato o acuerdo de la persona. Otros contratos o acuerdos que continúan por un período definido después del final del empleo del individuo también pueden contener responsabilidades de seguridad de la información.

Los cambios de responsabilidad o empleo deberían gestionarse como la terminación de la responsabilidad o empleo actual combinada con el inicio de la nueva responsabilidad o empleo.

Las funciones y responsabilidades de seguridad de la información que tenga cualquier persona que deje o cambie de puesto deberían identificarse y transferirse a otra persona.

debería establecerse un proceso para la comunicación de los cambios y de los procedimientos operativos al personal, a otras partes interesadas y a las personas de contacto pertinentes (por ejemplo, a clientes y proveedores).

El proceso de terminación o cambio de empleo también debería aplicarse al personal externo (es decir, proveedores) cuando se produce una terminación del personal, del contrato o del puesto con la organización, o cuando hay un cambio de puesto dentro de la organización.

Otra información

En muchas organizaciones, la función de recursos humanos generalmente es responsable del proceso general de terminación y trabaja junto con el gerente supervisor de la persona en transición para administrar los aspectos de seguridad de la información de los procedimientos relevantes. En el caso de personal proporcionado a través de una parte externa (por ejemplo, a través de un proveedor), este proceso de terminación lo lleva a cabo la parte externa de acuerdo con el contrato entre la organización y la parte externa.

6.6 Acuerdos de confidencialidad o no divulgación

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_en_recursos_humanos #Protección_de_información #Relaciones_con_proveedores	#Gobernanza_y_Eco-sistema

Control

Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deberían ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

Propósito

Para mantener la confidencialidad de la información accesible por el personal o partes externas.

Guía

Los acuerdos de confidencialidad o de no divulgación deberían abordar el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. En función de los requisitos de seguridad de la información de una organización, los términos de los acuerdos deberían determinarse 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 los requisitos para los acuerdos de confidencialidad o no divulgación, se deberían considerar los siguientes elementos:

a) una definición de la información a proteger (por ejemplo, información confidencial);

b) la duración esperada de un acuerdo, incluidos los casos en los que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté disponible públicamente;

c) las acciones requeridas cuando se termina un acuerdo;

d) las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada;

e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial;

f) el uso permitido de la información confidencial y los derechos del firmante para usar la información;

g) el derecho a auditar y monitorear actividades que involucren información confidencial para circunstancias altamente sensibles;

h) el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial;

i) los términos para la devolución o destrucción de la información al término del contrato;

j) las acciones previstas a tomar en caso de incumplimiento del acuerdo.

La organización debería tener en cuenta la conformidad con los acuerdos de confidencialidad y no divulgación para la jurisdicción a la que se aplican (véase 5.31, 5.32, 5.33, 5.34).

Los requisitos para los acuerdos de confidencialidad y no divulgación deberían revisarse periódicamente y cuando ocurran cambios que influyan en estos requisitos.

Otra información

Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad de proteger, usar y divulgar la información de manera responsable y autorizada.

6.7 Trabajo remoto

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información #Seguridad_física #Seguridad_de_sistemas_y_redes	#Protección

Control

Se deberían implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información accedido, procesado o almacenado fuera de las instalaciones de la organización.

Propósito

Para garantizar la seguridad de la información cuando el personal está trabajando de forma remota.

Guía

El trabajo remoto ocurre cuando el personal de la organización trabaja desde un lugar fuera de las instalaciones de la organización, accediendo a la información ya sea en forma impresa o electrónica a través de equipos de TIC. Los entornos de trabajo remoto incluyen los denominados "teletrabajo", "teletrabajo", "lugar de trabajo flexible", "entornos de trabajo virtuales" y "mantenimiento remoto".

Las organizaciones que permiten actividades de trabajo a distancia deberían emitir una política específica sobre el tema del trabajo a distancia que defina las condiciones y restricciones pertinentes. Cuando se considere aplicable, se deberían considerar los siguientes asuntos:

NOTA: Es posible que no todas las recomendaciones en este control puedan ser aplicadas debido a la legislación local y regulaciones en diferentes jurisdicciones.

a) la seguridad física existente o propuesta del sitio de trabajo remoto, teniendo en cuenta la seguridad física de la ubicación y el entorno local, incluidas las diferentes jurisdicciones legales donde se encuentra el personal;

b) reglas y mecanismos de seguridad para el entorno físico remoto, como archivadores con cerradura, transporte seguro entre ubicaciones y reglas para el acceso remoto, escritorio despejado, impresión y eliminación de información y otros activos asociados, e informes de eventos de seguridad de la información (véase 6.8);

c) los entornos físicos de trabajo remoto esperados;

d) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de la organización, la sensibilidad de la información a la que se accederá y pasará por el enlace de comunicación y la sensibilidad de los sistemas y aplicaciones;

e) el uso de acceso remoto, como acceso de escritorio virtual que soporta el procesamiento y almacenamiento de información en equipos de propiedad privada;

f) la amenaza de acceso no autorizado a información o recursos de otras personas en el lugar lugar de trabajo remoto (por ejemplo, familia y amigos);

g) la amenaza de acceso no autorizado a información o recursos de otras personas en lugares públicos;

h) el uso de redes domiciliarias y redes públicas, y requisitos o restricciones en la configuración de servicios de redes inalámbricas;

i) uso de medidas de seguridad, como firewalls y protección contra malware;

j) mecanismos seguros para implementar e inicializar sistemas de forma remota;

k) mecanismos seguros de autenticación y habilitación de privilegios de acceso teniendo en cuenta la vulnerabilidad de los mecanismos de autenticación de un solo factor donde se permite el acceso remoto a la red de la organización.

Las directrices y medidas a considerar deberían incluir:

a) la provisión de equipos y muebles de almacenamiento adecuados para las actividades de trabajo remoto, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;

b) una definición del trabajo permitido, la clasificación de la información que puede ser mantenida y los sistemas y servicios internos a los que el trabajador remoto está autorizado a acceder;

c) la provisión de capacitación para quienes trabajan a distancia y quienes brindan apoyo. Esto debería incluir cómo realizar negocios de manera segura mientras se trabaja de forma remota;

d) la provisión de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto, como los requisitos sobre bloqueos de pantalla del dispositivo y temporizadores de inactividad; la habilitación del seguimiento de la ubicación del dispositivo; instalación de capacidades de borrado remoto;

e) seguridad física;

f) reglas y orientación sobre el acceso de familiares y visitantes a equipos e información;

g) la provisión de soporte y mantenimiento de hardware y software;

h) la provisión de seguros;

i) los procedimientos de respaldo y continuidad del negocio;

j) auditoría y seguimiento de la seguridad;

k) revocación de autorización y derechos de acceso y devolución de equipos cuando el trabajo a distancia se dan por terminadas las actividades.

Otra información

No hay otra información.

6.8 Reporte de eventos de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

La organización debería proporcionar un mecanismo para que el personal informes eventos de seguridad de la información observados o bajo sospecha a través de los canales apropiados de manera oportuna.

Propósito

Para respaldar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que puedan ser identificados por el personal.

Guía

Todo el personal y los usuarios deberían ser conscientes de su responsabilidad de informar los eventos de seguridad de la información tan pronto como sea posible para minimizar el efecto de los incidentes de seguridad de la información.

También deberían conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se deberían informar los eventos. El mecanismo de presentación de informes debería ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, violaciones y vulnerabilidades.

Las situaciones por considerar para el reporte de eventos de seguridad de la información incluyen:

a) control de seguridad de la información ineficaz;

b) incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información;

c) errores humanos;

d) incumplimiento de la política de seguridad de la información, políticas de tópico específico o normas aplicables;

e) incumplimientos de las medidas de seguridad física;

f) cambios del sistema que no han pasado por el proceso de gestión de cambios;

g) mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware;

h) infracciones de acceso;

i) vulnerabilidades;

j) sospecha de infección por malware.

Se debería advertir al personal y a los usuarios que no intenten probar vulnerabilidades de seguridad de la información sospechosas. Las vulnerabilidades de prueba pueden interpretarse como un mal uso potencial del sistema y también pueden causar daños al sistema o servicio de información, y pueden corromper u ocultar la evidencia digital. En última instancia, esto puede resultar en responsabilidad legal para la persona que realiza la prueba.

Otra información

Consulte la serie ISO/IEC 27035 para obtener información adicional.

7 Controles físicos

7.1 Perímetros de seguridad física

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#proteger	#Seguridad_física	#protección

Control

Los perímetros de seguridad deberían definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.

Propósito

Para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.

Guía

Se deberían considerar e implementar las siguientes pautas cuando sea apropiado para los perímetros de seguridad física:

a) definir los perímetros de seguridad y la ubicación y resistencia de cada uno de los perímetros de acuerdo con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro;

b) tener perímetros físicamente sólidos para un edificio o sitio que contenga instalaciones de procesamiento de información (es decir, no debería haber huecos en el perímetro o áreas donde un robo pueda ocurrir fácilmente). Los techos, paredes, techos y pisos exteriores del sitio deberían ser de construcción sólida y todas las puertas externas deberían estar adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras). Las puertas y ventanas deberían cerrarse con llave cuando estén desatendidas y se debería considerar la protección externa para las ventanas, particularmente a nivel del suelo; también deberían tenerse en cuenta los puntos de ventilación;

c) Alarmas, monitoreos y probar todas las puertas cortafuegos en un perímetro de seguridad en conjunto con los muros para establecer el nivel de resistencia requerido de acuerdo con las normas adecuadas. deberían funcionar a prueba de fallos.

Otra información

La protección física se puede lograr creando una o más barreras físicas alrededor de las instalaciones de la organización y las instalaciones de procesamiento de información.

Un área segura puede ser una oficina con cerradura o varias habitaciones rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarias barreras y perímetros adicionales para controlar el 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 puedan reforzarse durante situaciones de mayor amenaza.

7.2 Ingreso físico

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_identidades_y_acceso	#Protección

Control

Las áreas seguras deberían estar protegidas por controles de entrada y puntos de acceso adecuados.

Propósito

Para garantizar que solo se produzca el acceso físico autorizado a la información de la organización y otros activos asociados.

Guía

Generalidades

Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a las instalaciones deberían estar controlados y, si es posible, aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Deberían tenerse en cuenta las siguientes pautas:

a) restringir el acceso a los sitios y edificios solo al personal autorizado. El proceso para la gestión de los derechos de acceso a las áreas físicas debería incluir la provisión, revisión periódica, actualización y revocación de autorizaciones (véase 5.18);

b) mantener y monitorear de manera segura un libro de registro físico o una pista de auditoría electrónica de todos los accesos y proteger todos los registros (véase 5.33) y la información de autenticación sensible;

c) establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, autenticación biométrica o de dos factores, como una tarjeta de acceso y un PIN secreto. Se deberían considerar las puertas de seguridad dobles para el acceso a áreas sensibles;

d) establecer un área de recepción monitoreada por el personal u otros medios para controlar el acceso físico al sitio o edificio;

e) inspeccionar y examinar las pertenencias personales del personal y las partes interesadas a la entrada y salida;

NOTA: Pueden existir leyes y regulaciones locales con respecto a la posibilidad de inspeccionar pertenencias personales.

f) exigir que todo el personal y las partes interesadas usen algún tipo de identificación visible y que notifiquen inmediatamente al personal de seguridad si encuentran visitantes sin escolta y cualquier persona que no lleve una identificación visible. deberían considerarse insignias fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes;

g) otorgar al personal del proveedor acceso restringido a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario. Este acceso debería ser autorizado y monitoreado;

h) prestar especial atención a la seguridad del acceso físico en el caso de edificios con activos para múltiples organizaciones;

i) diseñar medidas de seguridad física para que puedan fortalecerse cuando aumente la probabilidad de incidentes físicos;

j) asegurar otros puntos de entrada, como salidas de emergencia, del acceso no autorizado;

k) establecer un proceso de gestión de claves para garantizar la gestión de las claves físicas o la información de autenticación (por ejemplo, códigos de bloqueo, cerraduras de combinación para oficinas, salas e instalaciones, como armarios de llaves) y garantizar un libro de registro o una auditoría anual de claves y ese acceso a las claves físicas o la información de autenticación se controla (consulte 5.17 para obtener más orientación sobre la información de autenticación).

Visitantes

Deberían tenerse en cuenta las siguientes pautas:

a) autenticar la identidad de los visitantes por un medio adecuado;

b) registrar la fecha y hora de entrada y salida de los visitantes;

c) solo otorgar acceso a visitantes para fines específicos autorizados y con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia;

d) supervisar a todos los visitantes, a menos que se otorgue una excepción explícita.

Áreas de carga y descarga y de material entrante

Deberían tenerse en cuenta las siguientes pautas:

a) restringir el acceso a las áreas de entrega y carga desde el exterior del edificio al personal identificado y autorizado;

b) diseñar las áreas de entrega y carga para que las entregas se puedan cargar y descargar sin que el personal de entrega tenga acceso no autorizado a otras partes del edificio;

c) asegurar las puertas exteriores de las áreas de entrega y carga cuando se abren las puertas de las áreas restringidas;

d) inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que se muevan desde las áreas de entrega y carga;

e) registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos (véase 5.9 y 7.10) al ingresar al sitio;

f) separar físicamente los envíos entrantes y salientes, cuando sea posible;

g) inspeccionar las entregas entrantes en busca de evidencia de manipulación en el camino. Si se descubre una manipulación, se debería informar de inmediato al personal de seguridad.

Otra información

No hay otra información.

7.3 Asegurar oficinas, salas e instalaciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Se debería diseñar e implementar la seguridad física para oficinas, salas e instalaciones.

Propósito

Para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en oficinas, salas e instalaciones.

Guía

Se deberían considerar las siguientes pautas para asegurar oficinas, salas e instalaciones:

a) ubicar las instalaciones críticas para evitar el acceso del público;

b) cuando corresponda, asegurar que los edificios sean discretos y den una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, identificando la presencia de actividades de procesamiento de información;

c) configurar instalaciones para evitar que información o actividades confidenciales sean visibles y audibles desde el exterior. También debería considerarse apropiado el blindaje electromagnético;

d) no poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen ubicaciones de instalaciones de procesamiento de información confidencial.

Otra información

No hay otra información.

7.4 Supervisión de la seguridad física

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #detectar	#Seguridad_física	#Protección #Defensa

Control

Las instalaciones deberían ser monitoreadas continuamente para detectar accesos físicos no autorizados.

Propósito

Detectar y disuadir el acceso físico no autorizado.

Guía

Las instalaciones físicas deberían ser monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de monitoreo de video como televisión de circuito cerrado y software de administración de información de seguridad física, ya sea administrado internamente o por un proveedor de servicios de monitoreo.

El acceso a los edificios que albergan sistemas críticos debería monitorearse continuamente para detectar accesos no autorizados o comportamientos sospechosos mediante:

a) instalar sistemas de monitoreo de video, como circuito cerrado de televisión, para ver y grabar el acceso a áreas sensibles dentro y fuera de las instalaciones de una organización;

b) instalar, de acuerdo con las normas aplicables pertinentes, y probar periódicamente 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 donde se pueda hacer o romper un contacto (como ventanas y puertas y debajo de objetos) para usarlo como alarma de pánico;

2) detectores de movimiento basados en tecnología infrarroja que disparan una alarma cuando un objeto pasa por su campo de visión;

3) instalar sensores sensibles al sonido de cristales rotos que se pueden utilizar para activar una alarma para alertar al personal de seguridad;

c) usar esas alarmas para cubrir todas las puertas externas y ventanas accesibles. Las áreas desocupadas deberían estar alarmadas en todo momento; también se debería proporcionar cobertura para otras áreas (por ejemplo, salas de computadoras o de comunicaciones).

El diseño de los sistemas de monitoreo debería mantenerse confidencial porque la divulgación puede facilitar robos no detectados.

Los sistemas de monitoreo deberían protegerse del acceso no autorizado para evitar que personas no autorizadas accedan a la información de vigilancia, como las transmisiones de video, o que los sistemas se deshabiliten de forma remota.

El panel de control del sistema de alarma debería colocarse en una zona de alarma y, para las alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que activa la alarma. El panel de control y los detectores deberían tener mecanismos a prueba de manipulaciones. El sistema debería probarse periódicamente para asegurarse de que funciona según lo previsto, especialmente si sus componentes funcionan con batería.

Cualquier mecanismo de monitoreo y grabación debería utilizarse teniendo en cuenta las leyes y regulaciones locales, incluida la protección de datos y la legislación de protección de IIP, especialmente con respecto al monitoreo del personal y los períodos de retención de videos grabados.

Otra información

No hay otra información.

7.5 Protección contra amenazas físicas y ambientales

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Se debería diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

Propósito

Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.

Guía

Se deberían realizar evaluaciones de riesgo para identificar las posibles consecuencias de las amenazas físicas y ambientales antes de comenzar las operaciones críticas en un sitio físico y a intervalos regulares. Se deberían implementar las salvaguardas necesarias y se deberían monitorear los cambios en las amenazas. Se debería obtener asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y ambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos.

La ubicación física y la construcción de los locales deberían tener en cuenta:

a) topografía local, como elevación apropiada, cuerpos de agua y fallas tectónicas;

b) amenazas urbanas, tales como lugares con un perfil alto para atraer disturbios políticos, actividades delictivas o ataques terroristas.

Con base en los resultados de la evaluación de riesgos, se deberían identificar las amenazas físicas y ambientales relevantes y se deberían considerar los controles apropiados en los siguientes contextos como ejemplos:

a) incendio: instalación y configuración de sistemas capaces de detectar incendios en una etapa temprana para enviar alarmas o activar sistemas de extinción de incendios a fin de evitar daños por incendios en los medios de almacenamiento y los sistemas de procesamiento de información relacionados. La extinción de incendios debería realizarse utilizando la sustancia más adecuada con respecto al entorno circundante (por ejemplo, gas en espacios confinados);

b) inundaciones: instalación de sistemas capaces de detectar inundaciones en una etapa temprana debajo de los pisos de áreas que contienen medios de almacenamiento o sistemas de procesamiento de información. Deberían estar disponibles bombas de agua o medios equivalentes en caso de que se produzca una inundación;

c) sobretensiones eléctricas: adopción de sistemas capaces de proteger los sistemas de información del servidor y del cliente contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de tales eventos;

d) explosivos y armas: realizar inspecciones aleatorias por la presencia de explosivos o armas en el personal, vehículos o mercancías que ingresan a las instalaciones de procesamiento de información sensible.

Otra información

Las cajas fuertes u otras formas de instalaciones de almacenamiento seguro pueden proteger la información almacenada en ellas contra desastres como incendios, terremotos, inundaciones o explosiones.

Las organizaciones pueden considerar los conceptos de prevención del delito a través del diseño ambiental al diseñar los controles para proteger su entorno y reducir las amenazas urbanas. Por ejemplo, en lugar de utilizar bolardos, las estatuas o los elementos acuáticos pueden servir como elemento y como barrera física.

7.6 Trabajo en áreas seguras

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Deberían diseñarse e implementarse medidas de seguridad para trabajar en áreas seguras.

Propósito

Para proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

Guía

Las medidas de seguridad para trabajar en áreas seguras deberían aplicarse a todo el personal y cubrir todas las actividades que tienen lugar en el área segura.

Deberían tenerse en cuenta las siguientes pautas:

a) concienciar al personal solo de la existencia o de las actividades dentro de un área segura según sea necesario;

b) evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas;

c) cerrar físicamente e inspeccionar periódicamente las áreas seguras vacías;

d) no permitir equipos de grabación de fotografías, video, audio u otros, como cámaras, en dispositivos terminales de usuario, a menos que estén autorizados;

e) controlar apropiadamente el transporte y uso de dispositivos terminales de usuario en áreas seguras;

f) publicar los procedimientos de emergencia de una manera fácilmente visible o accesible.

Otra información

No hay otra información.

7.7 Escritorio y pantalla limpios

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física	#Protección

Control

deberían definirse y aplicarse adecuadamente reglas de escritorio limpio de papeles y medios de almacenamiento extraíbles y reglas de pantalla limpia en las instalaciones de procesamiento de información.

Propósito

Reducir los riesgos de acceso no autorizado, pérdida y daño a la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario laboral normal.

Guía

La organización debería establecer y comunicar una política de tópico específico sobre escritorios y una pantalla limpia a todas las partes interesadas relevantes.

Deberían tenerse en cuenta las siguientes pautas:

a) bloquear la información comercial sensible o crítica (por ejemplo, en papel o en un medio de almacenamiento electrónico) (idealmente en una caja fuerte, gabinete u otra forma de mobiliario de seguridad) cuando no sea necesario, especialmente cuando la oficina está desocupada;

b) proteger los dispositivos terminales de los usuarios mediante cerraduras con llave u otros medios de seguridad cuando no estén en uso o 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 de usuario cuando están desatendidos. Todas las computadoras y sistemas deberían configurarse con una función de tiempo de espera o cierre de sesión automático;

d) hacer que el creador recopile los resultados de las impresoras o dispositivos multifunción de inmediato. El uso de impresoras con función de autenticación, por lo que los creadores son los únicos que pueden obtener sus impresiones y solo cuando están al lado de la impresora;

e) almacenar de forma segura los documentos y los medios de almacenamiento extraíbles que contienen información sensible y, cuando ya no se necesiten, desecharlos mediante mecanismos de eliminación seguros;

f) establecer y comunicar reglas y orientación para la configuración de ventanas emergentes en las pantallas (por ejemplo, apagar los nuevos mensajes emergentes de correo electrónico y mensajes, si es posible, durante presentaciones, compartir pantalla o en un área pública);

g) borrar información sensible o crítica en pizarras y otros tipos de pantallas cuando ya no se necesiten.

La organización debería tener procedimientos establecidos al desocupar las instalaciones, incluida la realización de un barrido final antes de partir para garantizar que los activos de la organización no se queden atrás (por ejemplo, documentos caídos detrás de cajones o muebles).

Otra información

No hay otra información.

7.8 Ubicación y protección de los equipos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

El equipo debería estar ubicado de forma segura y protegida.

Propósito

Reducir los riesgos de las amenazas físicas y ambientales, y del acceso no autorizado y los daños.

Guía

Se deberían considerar las siguientes pautas para proteger el equipo:

a) ubicar el equipo para minimizar el acceso innecesario a las áreas de trabajo y evitar el acceso no autorizado;

b) ubicar cuidadosamente las instalaciones de procesamiento de información que manejan datos sensibles para reducir el riesgo de que personas no autorizadas vean la información durante su uso;

c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales [por ejemplo, robo, incendio, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo];

d) establecer pautas para comer, beber y fumar en las proximidades de las instalaciones de procesamiento de información;

e) monitorear las condiciones ambientales, como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente el funcionamiento de las instalaciones de procesamiento de información;

f) aplicar protección contra rayos a todos los edificios y colocar filtros de protección contra rayos en todas las líneas de alimentación y comunicaciones entrantes;

g) considerar el uso de métodos especiales de protección, como membranas de teclado, para equipos en entornos industriales;

h) proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética;

i) separar físicamente las instalaciones de procesamiento de información administradas por la organización de aquellas no administradas por la organización.

Otra información

No hay otra información.

7.9 Seguridad de los activos fuera de las instalaciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Los activos fuera del sitio deberían protegerse.

Propósito

Para evitar pérdidas, daños, robos o comprometer los activos externos y la interrupción de las operaciones de la organización.

Guía

Cualquier dispositivo que se use fuera de las instalaciones de la organización y que almacene o procese información (por ejemplo, un dispositivo móvil), incluidos los dispositivos de propiedad de la organización y los dispositivos de propiedad privada y utilizados en nombre de la organización (TTPD), necesita protección. El uso de estos dispositivos debería ser autorizado por la gerencia.

Se deberían considerar las siguientes pautas para la protección de equipos que almacenan o procesan información fuera de las instalaciones de la organización:

a) no dejar equipos y medios de almacenamiento retirados de las instalaciones sin vigilancia en lugares públicos y no seguros;

b) observar las instrucciones de los fabricantes para proteger el equipo en todo momento (por ejemplo, protección contra la exposición a campos electromagnéticos fuertes, agua, calor, humedad, polvo);

c) cuando se transfiera equipo fuera de las instalaciones entre diferentes personas o partes interesadas, llevar un registro que defina la cadena de custodia del equipo, incluyendo al menos los nombres y organizaciones de los responsables del equipo. La información que no necesita ser transferida con el activo debería eliminarse de forma segura antes de la transferencia;

d) cuando sea necesario y práctico, exigir autorización para retirar equipos y medios de las instalaciones de la organización y mantener un registro de dichas retiradas a fin de mantener una pista de auditoría (véase 5.14);

e) protección contra la visualización de información en un dispositivo (por ejemplo, un dispositivo móvil o una computadora portátil) en el transporte público y los riesgos asociados con la navegación lateral;

f) implementación de rastreo de ubicación y capacidad para borrar dispositivos de forma remota.

La instalación permanente de equipos fuera de las instalaciones de la organización [como antenas y cajeros automáticos (ATM)] puede estar sujeta a un mayor riesgo de daño, robo o escuchas.

Estos riesgos pueden variar considerablemente entre ubicaciones y deberían tenerse en cuenta para determinar las medidas más adecuadas. Se deberían tener en cuenta las siguientes pautas al ubicar este equipo fuera de las instalaciones de la organización:

a) supervisión de la seguridad física (véase 7.4);

b) protección contra amenazas físicas y ambientales (véase 7.5);

c) controles de acceso físico y a prueba de manipulaciones;

d) controles de acceso lógico.

Otra información

Más información sobre otros aspectos de la protección de equipos de procesamiento y almacenamiento de información y dispositivos terminales de usuario se puede encontrar en 8.1 y 6.7.

7.10 Medios de almacenamiento

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Los medios de almacenamiento deberían gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación.

Propósito

Para garantizar solo la divulgación, modificación, eliminación o destrucción autorizadas de la información en los medios de almacenamiento.

Guía

Medios de almacenamiento extraíbles

Deberían tenerse en cuenta las siguientes pautas para la gestión de medios de almacenamiento extraíbles:

a) establecer una política de tema específico sobre la gestión de medios de almacenamiento extraíbles y comunicar dicha política de tema específico a cualquiera que utilice o manipule medios de almacenamiento extraíbles;

b) cuando sea necesario y práctico, exigir autorización para retirar los medios de almacenamiento de la organización y mantener un registro de dichas retiradas para mantener una pista de auditoría;

c) almacenar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes;

d) si la confidencialidad o integridad de la información son consideraciones importantes, utilizar técnicas criptográficas para proteger la información en los medios de almacenamiento extraíbles;

e) mitigar el riesgo de degradación de los medios de almacenamiento mientras la información almacenada todavía es necesaria, transfiriendo la información a medios de almacenamiento nuevos antes de que se vuelva ilegible;

f) almacenar múltiples copias de información valiosa en medios de almacenamiento separados para reducir aún más el riesgo de daño o pérdida de información coincidente;

g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;

h) habilitar solo puertos de medios de almacenamiento extraíbles (por ejemplo, ranuras para tarjetas SD y puertos USB) si existe una razón organizativa para su uso;

i) cuando sea necesario utilizar medios de almacenamiento extraíbles, supervisar la transferencia de información a dichos medios de almacenamiento;

j) la información puede ser vulnerable a acceso no autorizado, uso indebido o corrupción durante el transporte físico, por ejemplo, al enviar medios de almacenamiento a través del servicio postal o de mensajería.

En este control, los medios incluyen documentos en papel. Al transferir medios de almacenamiento físico, aplique las medidas de seguridad en 5.14.

Reutilización o eliminación segura

Deberían establecerse procedimientos para la reutilización o eliminación segura de los medios de almacenamiento a fin de minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación segura de los medios de almacenamiento que contienen información confidencial deberían ser proporcionales a la sensibilidad de esa información. deberían tenerse en cuenta los siguientes elementos:

a) si los medios de almacenamiento que contienen información confidencial necesitan ser reutilizados dentro de la organización, borrando de forma segura los datos o formateando los medios de almacenamiento antes de su reutilización (véase 8.10);

b) deshacerse de los medios de almacenamiento que contienen información confidencial de forma segura cuando ya no se necesitan (por ejemplo, destruyendo, triturando o borrando de forma segura el contenido);

c) disponer de procedimientos para identificar los elementos que pueden requerir una eliminación segura;

d) muchas organizaciones ofrecen servicios de recolección y eliminación de medios de almacenamiento. Se debería tener cuidado al seleccionar un proveedor externo adecuado con los controles y la experiencia adecuados;

e) registrar la eliminación de artículos sensibles para mantener una pista de auditoría;

f) al acumular medios de almacenamiento para su eliminación, teniendo en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se vuelva sensible.

Se debería realizar una evaluación de riesgos en los dispositivos dañados que contienen datos confidenciales para determinar si los elementos deberían destruirse físicamente en lugar de enviarse para su reparación o desecharse (véase 7.14).

Otra información

Cuando la información confidencial en los medios de almacenamiento no está encriptada, se debería considerar la protección física adicional de los medios de almacenamiento.

7.11 Servicios de suministro

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #detectar	#Seguridad_física	#Protección

Control

Las instalaciones de procesamiento de información deberían protegerse de cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

Propósito

Para evitar la pérdida, el daño o el compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a la falla y la interrupción de los servicios públicos de apoyo.

Guía

Las organizaciones dependen de los servicios públicos (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para respaldar sus instalaciones de procesamiento de información. Por tanto, la organización debería:

a) asegurarse de que el equipo de apoyo a los servicios públicos esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente;

b) asegurar que las empresas de servicios públicos se evalúen periódicamente por su capacidad para cumplir con el crecimiento del negocio y las interacciones con otras empresas de servicios de apoyo;

c) asegurarse de que el equipo de apoyo a los servicios públicos se inspeccione y pruebe periódicamente para garantizar su correcto funcionamiento;

d) si es necesario, activar alarmas para detectar fallas en los servicios públicos;

e) si es necesario, asegúrese de que las empresas de servicios públicos tengan múltiples alimentaciones con enrutamiento físico diverso;

f) asegurarse de que el equipo de apoyo a los servicios públicos esté en una red separada de las instalaciones de procesamiento de información si está conectado a una red;

g) asegurarse de que el equipo de apoyo a los servicios públicos esté conectado a Internet solo cuando sea necesario y solo de manera segura.

Se deberían proporcionar luces y comunicaciones de emergencia. Los interruptores de emergencia y las válvulas para cortar la energía, el agua, el gas u otros servicios públicos deberían ubicarse cerca de las salidas de emergencia o las salas de equipos. Los datos de contacto de emergencia deberían registrarse y estar disponibles para el personal en caso de un apagón.

Otra información

Se puede obtener redundancia adicional para la conectividad de la red mediante múltiples rutas de más de un proveedor de servicios públicos.

7.12 Seguridad del cableado

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Los cables que transportan energía, datos o servicios de información de apoyo deberían protegerse contra intercepciones, interferencias o daños.

Propósito

Para evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

Guía

Se deberían considerar las siguientes pautas para la seguridad del cableado:

a) las líneas de energía y telecomunicaciones hacia las instalaciones de procesamiento de información que sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como un protector de cable de piso y un poste de servicios públicos; si los cables están bajo tierra, protegiéndolos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia);

b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;

c) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:

1) instalación de conductos blindados y habitaciones o cajas cerradas y alarmas en los puntos de inspección y terminación;

2) uso de blindaje electromagnético para proteger los cables;

3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables;

4) acceso controlado a paneles de conexiones y salas de cables (por ejemplo, con llaves mecánicas o PIN);

5) uso de cables de fibra óptica;

d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

Se debería buscar el asesoramiento de un especialista sobre cómo gestionar los riesgos derivados de incidentes de cableado o averías.

Otra información

A veces, el cableado de energía y telecomunicaciones son recursos compartidos para más de una organización que ocupa instalaciones que comparten el mismo edificio.

7.13 Mantenimiento de equipos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección #Resiliencia

Control

El equipo debería mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

Propósito

Para evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.

Guía

Se deberían considerar las siguientes pautas para el mantenimiento del equipo:

a) mantener el equipo de acuerdo con las especificaciones y la frecuencia de servicio recomendadas por el proveedor;

b) implementación y seguimiento de un programa de mantenimiento por parte de la organización;

c) solo personal de mantenimiento autorizado que realice reparaciones y mantenimiento de equipos;

d) mantener registros de todas las fallas, sospechadas o reales, y de todo el mantenimiento preventivo y correctivo;

e) implementar controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización; someter al personal de mantenimiento a un acuerdo de confidencialidad adecuado;

f) supervisar al personal de mantenimiento cuando realiza el mantenimiento en el sitio;

g) autorizar y controlar el acceso para mantenimiento remoto;

h) aplicar medidas de seguridad para los activos fuera de las instalaciones (véase 7.9) si el equipo que contiene información se retira de las instalaciones para su mantenimiento;

i) cumplir con todos los requisitos de mantenimiento impuestos por el seguro;

j) antes de volver a poner el equipo en funcionamiento después del mantenimiento, inspeccionarlo para asegurarse de que no haya sido manipulado y esté funcionando correctamente;

k) aplicar medidas para la eliminación segura o la reutilización del equipo (véase 7.14) si se determina que el equipo debería eliminarse.

Otra información

El equipo incluye componentes técnicos de instalaciones de procesamiento de información, UPS y baterías, generadores de energía, alternadores y convertidores de energía, sistemas de detección de intrusión física y alarmas, detectores de humo, extintores de incendios, aire acondicionado y ascensores.

7.14 Eliminación o reutilización segura de equipos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Los elementos del equipo que contienen medios de almacenamiento deberían verificarse para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Propósito

Para evitar la fuga de información de los equipos que se desecharán o reutilizarán.

Guía

El equipo debería verificarse para asegurarse de que los medios de almacenamiento estén o no contenidos antes de su eliminación o reutilización.

Los medios de almacenamiento que contienen información confidencial o protegida por derechos de autor deberían destruirse físicamente o la información debería destruirse, eliminarse o sobrescribirse utilizando técnicas para hacer que la información original no se pueda recuperar en lugar de utilizar la función de eliminación estándar. Consulte 7.10 para obtener una guía detallada sobre la eliminación segura de los medios de almacenamiento y 8.10 para obtener una guía sobre la eliminación de información.

Las etiquetas y marcas que identifican a la organización o que indican la clasificación, el propietario, el sistema o la red deberían eliminarse antes de su eliminación, incluida la reventa o la donación a organizaciones benéficas.

La organización debería considerar la eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia, al final del contrato de arrendamiento o al mudarse de las instalaciones. Esto depende de factores como:

a) su contrato de arrendamiento para devolver la instalación a su estado original;

b) minimizar el riesgo de dejar sistemas con información confidencial para el próximo inquilino (por ejemplo, listas de acceso de usuarios, archivos de video o imágenes);

c) la capacidad de reutilizar los 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 deberían destruirse físicamente en lugar de enviarse para su reparación o desecharse. La información puede verse comprometida por la eliminación descuidada o la reutilización del equipo.

Además de la eliminación segura del disco, el cifrado de disco completo reduce el riesgo de divulgación de información confidencial cuando el equipo se desecha o se vuelve a implementar, siempre que:

a) el proceso de cifrado es lo suficientemente sólido y cubre todo el disco (incluido el espacio libre, los archivos de intercambio);

b) las claves criptográficas son lo suficientemente largas para resistir ataques de fuerza bruta;

c) las claves criptográficas se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para obtener más consejos sobre criptografía, consulte 8.24.

Las técnicas para sobrescribir de forma segura los medios de almacenamiento difieren según la tecnología de los medios de almacenamiento y el nivel de clasificación de la información en los medios de almacenamiento. Las herramientas de sobreescritura deberían revisarse para asegurarse de que sean aplicables a la tecnología de los medios de almacenamiento.

Consulte ISO/IEC 27040 para obtener detalles sobre los métodos para higienizar los medios de almacenamiento.

8 Controles tecnológicos

8.1 Dispositivos de punto final de usuario

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Protección

Control

La información almacenada, procesada o accesible a través de dispositivos terminales de usuario debería protegerse.

Propósito

Para proteger la información contra los riesgos introducidos por el uso de dispositivos terminales de usuario.

Guía

Generalidades

La organización debería establecer una política de tema específico sobre la configuración segura y el manejo de los dispositivos de los terminales de los usuarios. La política de tópico específico debería comunicarse a todo el personal relevante y considerar lo siguiente:

a) el tipo de información y el nivel de clasificación que los dispositivos de punto final del usuario pueden manejar, procesar, almacenar o soportar;

b) registro de dispositivos de punto final de usuario;

c) requisitos de protección física;

d) restricción de la instalación de software (por ejemplo, controlado de forma remota por los administradores del sistema);

e) requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para la aplicación de actualizaciones (por ejemplo, actualización automática activa);

f) reglas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones (por ejemplo, que requiera el uso de un cortafuegos personal);

g) controles de acceso;

h) cifrado del dispositivo de almacenamiento;

i) protección contra malware;

j) desactivación, borrado o bloqueos remotos;

k) copias de seguridad;

l) uso de servicios web y aplicaciones web;

m) análisis del comportamiento del usuario final (véase 8.16);

n) el uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de desactivar puertos físicos (por ejemplo, puertos USB);

o) el uso de capacidades de partición, si es compatible con el dispositivo de punto final del usuario, que puede separar de forma segura la información de la organización y otros activos asociados (por ejemplo, software) de otra información y otros activos asociados en el dispositivo.

Se debería considerar si cierta información es tan sensible que solo se puede acceder a ella a través de los dispositivos de punto final del usuario, pero no se puede almacenar en dichos dispositivos. En tales casos, se pueden requerir protecciones técnicas adicionales en el dispositivo. Por ejemplo, asegurarse de que la descarga de archivos para trabajar sin conexión esté deshabilitada y que el almacenamiento local, como la tarjeta SD, esté deshabilitado.

En la medida de lo posible, las recomendaciones sobre este control deberían aplicarse mediante la gestión de la configuración (véase 8.9) o herramientas automatizadas.

Responsabilidad del usuario

Todos los usuarios deberían conocer los requisitos y procedimientos de seguridad para proteger los dispositivos terminales de los usuarios, así como sus responsabilidades para implementar dichas medidas de seguridad. Se debería advertir a los usuarios que:

a) cerrar sesión en sesiones activas y finalizar servicios cuando ya no se necesiten;

b) proteger los dispositivos terminales del usuario del uso no autorizado con un control físico (por ejemplo, cerradura de llave o cerraduras especiales) y un control lógico (por ejemplo, acceso con contraseña) cuando no estén en uso; no deje desatendidos los dispositivos que contienen información comercial importante, sensible o crítica;

c) usar dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas desprotegidas (por ejemplo, evite leer información confidencial si las personas pueden leer desde atrás, use filtros de pantalla de privacidad);

d) proteger físicamente los dispositivos terminales de los usuarios contra robos (por ejemplo, en automóviles y otras formas 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 (incluidos los seguros) y otros requisitos de seguridad de la organización para los casos de robo o pérdida de los dispositivos terminales de los usuarios.

Uso de dispositivos personales

Cuando la organización permita el uso de dispositivos personales (a veces conocidos como TTPD), además de la orientación proporcionada en este control, se debería considerar lo siguiente:

a) separación del uso personal y comercial de los dispositivos, incluido el uso de software para respaldar dicha separación y proteger los datos comerciales en un dispositivo privado;

b) proporcionar acceso a la información comercial solo después de que los usuarios hayan reconocido sus deberes (protección física, actualización de software, entre otros), renunciando a la propiedad de los datos comerciales, permitiendo la eliminación remota de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no está autorizado para utilizar el servicio. En tales casos, se debería considerar la legislación de protección de IIP;

c) políticas y procedimientos de temas específicos para prevenir disputas relacionadas con los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

d) acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que puede ser impedido por la legislación;

e) acuerdos de licencia de software que son tales que las organizaciones pueden ser responsables de la licencia de software de cliente en dispositivos terminales de usuario que sean propiedad privada del personal o de usuarios externos.

Conexiones inalámbricas

La organización debería establecer procedimientos para:

a) la configuración de conexiones inalámbricas en dispositivos (por ejemplo, deshabilitar protocolos vulnerables);

b) el uso de conexiones inalámbricas o por cable con el ancho de banda adecuado de acuerdo con las políticas de tópico específico relevante (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de software).

Otra información

Los controles para proteger la información en los dispositivos terminales del usuario dependen de si el dispositivo terminal del usuario se usa solo dentro de las instalaciones seguras de la organización y las conexiones de red, o si está expuesto a un aumento de las amenazas físicas y relacionadas con la red fuera de la organización.

Las conexiones inalámbricas para los dispositivos de punto final del usuario son similares a otros tipos de conexiones de red, pero tienen diferencias importantes que deberían tenerse en cuenta al identificar los controles. En particular, la copia de seguridad de la información almacenada en los dispositivos terminales del usuario a veces puede fallar debido al ancho de banda limitado de la red o porque los dispositivos terminales del usuario no están conectados en los momentos en que se programan las copias de seguridad.

Para algunos puertos USB, como USB-C, no es posible deshabilitar el puerto USB porque se utiliza para otros fines (por ejemplo, suministro de energía y salida de pantalla).

8.2 Derechos de acceso privilegiados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidades_y_acceso	#Protección

Control

La asignación y el uso de derechos de acceso privilegiado deberían restringirse y administrarse.

Propósito

Para garantizar que solo los usuarios autorizados, los componentes de software y los servicios reciban derechos de acceso privilegiado.

Guía

La asignación de derechos de acceso privilegiado debería controlarse a través de un proceso de autorización de acuerdo con la política de tópico específico relevante sobre control de acceso (véase 5.15). Se debería considerar lo siguiente:

a) identificar a los usuarios que necesitan derechos de acceso privilegiado para cada sistema o proceso (por ejemplo, sistemas operativos, sistemas de gestión de bases de datos y aplicaciones);

b) asignar derechos de acceso privilegiado a los usuarios según sea necesario y caso por evento de acuerdo con la política de tópico específico sobre control de acceso (véase 5.15) (es decir, solo a individuos con la competencia necesaria para llevar a cabo actividades que requieren privilegios acceso y con base en el requisito mínimo para sus roles funcionales);

c) mantener un proceso de autorización (es decir, determinar quién puede aprobar los derechos de acceso privilegiado, o no otorgar derechos de acceso privilegiado hasta que se complete el proceso de autorización) y un registro de todos los privilegios asignados;

d) definir e implementar requisitos para la expiración de los derechos de acceso privilegiado;

e) tomar medidas para que los usuarios conozcan sus derechos de acceso privilegiado y cuándo se encuentran en modo de acceso privilegiado. Las posibles medidas incluyen el uso de identidades de usuario específicas, configuraciones de interfaz de usuario o incluso equipos específicos;

f) los requisitos de autenticación para los derechos de acceso privilegiado pueden ser más altos que los requisitos para los derechos de acceso normales. Puede ser necesario volver a autenticar o incrementar la autenticación antes de trabajar con derechos de acceso privilegiados;

g) periódicamente, y después de cualquier cambio organizacional, revisar a los usuarios que trabajan con derechos de acceso privilegiado para verificar si sus deberes, roles, responsabilidades y competencias aún los califican para trabajar con derechos de acceso privilegiado (véase 5.18);

h) establecer reglas específicas para evitar el uso de ID de usuario de administración genéricos (como "root"), dependiendo de las capacidades de configuración de los sistemas. Gestionar y proteger la información de autenticación de dichas identidades (véase 5.17);

i) otorgar acceso privilegiado temporal solo durante el período de tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de otorgar derechos de acceso privilegiado permanentemente. Esto a menudo se conoce como procedimiento de ruptura de vidrio y, a menudo, se automatiza mediante tecnologías de administración de acceso con privilegios;

j) registrar todos los accesos privilegiados al sistema para fines de auditoría;

k) no compartir ni vincular identidades con derechos de acceso privilegiado a varias personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiado específicos. Las identidades se pueden agrupar (por ejemplo, definiendo un grupo de administradores) para simplificar la gestión de los derechos de acceso privilegiado;

l) solo usar identidades con derechos de acceso privilegiado para realizar tareas administrativas y no para tareas generales del día a día [es decir, revisar el correo electrónico, acceder a la web (los usuarios 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, una función o un proceso que permite la realización de actividades que los usuarios o procesos típicos no pueden realizar. Los roles de administrador del sistema generalmente requieren derechos de acceso privilegiados.

El uso inadecuado de los privilegios del administrador del sistema (cualquier característica o instalación de un sistema de información que permite al usuario anular los controles del sistema o de la aplicación) es un factor importante que contribuye a las fallas o brechas de los sistemas.

Se puede encontrar más información relacionada con la gestión del acceso y la gestión segura del acceso a la información y los recursos de tecnologías de la información y las comunicaciones en ISO/IEC 29146.

8.3 Restricción de acceso a la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidades_y_acceso	#Protección

Control

El acceso a la información y otros activos asociados debería restringirse de acuerdo con la política específica de tema establecida sobre control de acceso.

Propósito

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

Guía

El acceso a la información y otros activos asociados debería restringirse de acuerdo con las políticas establecidas para temas específicos. Se debería considerar lo siguiente para respaldar los requisitos de restricción de acceso:

a) No permitir el acceso a información sensible por identidades de usuario desconocidas o de forma anónima. El acceso público o anónimo solo debería otorgarse a ubicaciones de almacenamiento que no contengan información confidencial;

b) proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios;

c) controlar a qué datos puede acceder un usuario en particular;

d) controlar qué identidades o grupo de identidades tienen qué acceso, como lectura, escritura, eliminación y ejecución;

e) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones, datos de aplicaciones o sistemas sensibles.

Además, las técnicas y procesos de gestión de acceso dinámico para proteger la información sensible que tiene un alto valor para la organización deberían considerarse 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) quiere gestionar dinámicamente, en tiempo real, el uso y distribución de dicha información;

d) desea proteger dicha información contra cambios, copia y distribución (incluida la impresión) no autorizados;

e) quiere monitorear el uso de la información;

f) desea registrar cualquier cambio en dicha información que tenga lugar en caso de que se requiera una investigación futura.

Las técnicas de gestión de acceso dinámico deberían proteger la información a lo largo de su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) establecer reglas sobre la gestión del acceso dinámico en base a casos de uso específicos considerando:

   1) otorgar permisos de acceso basados en identidad, dispositivo, ubicación o aplicación;

   2) aprovechar el esquema de clasificación para determinar qué información debería protegerse con técnicas de gestión de acceso dinámico;

b) el establecimiento de procesos operativos, de seguimiento y presentación de informes y la infraestructura técnica de apoyo.

Los sistemas de gestión de acceso dinámico deberían proteger la información mediante:

a) requerir autenticación, credenciales adecuadas o un certificado para acceder a la información;

b) restringir el acceso, por ejemplo, a un período de tiempo específico (por ejemplo, después de una fecha determinada o hasta una fecha determinada);

c) utilizar cifrado para proteger la información;

d) definir los permisos de impresión de la información;

e) registrar quién accede a la información y cómo se utiliza la información;

f) generar alertas si se detectan intentos de hacer un mal uso de la información.

Otra información

Las técnicas de administración de acceso dinámico y otras tecnologías de protección de información dinámica pueden respaldar la protección de la información incluso cuando los datos se comparten más allá de la organización de origen, donde los controles de acceso tradicionales no se pueden hacer cumplir. Se puede aplicar a documentos, correos electrónicos u otros archivos que contienen información para limitar quién puede acceder al contenido y de qué manera. Puede ser a nivel granular y adaptarse a lo largo del ciclo de vida de la información.

Las técnicas de gestión de acceso dinámico no reemplazan la gestión de acceso clásica [por ejemplo, utilizando listas de control de acceso (LCA)], pero puede agregar 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. Ofrece una forma de controlar el acceso fuera del entorno de la organización. La respuesta a incidentes puede estar respaldada por técnicas de administración de acceso dinámico, ya que los permisos se pueden modificar o revocar en cualquier momento.

En ISO/IEC 29146 se proporciona información adicional sobre un marco para la gestión de acceso.

8.4 Acceso al código fuente

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidades_y_acceso #Seguridad_de_aplicaciones #Configuración_segura	#Protección

Control

El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debería administrarse adecuadamente.

Propósito

Para evitar la introducción de funciones no autorizadas, evite cambios no intencionales o maliciosos y mantenga la confidencialidad de la propiedad intelectual valiosa.

Guía

El acceso al código fuente y elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas de prueba y entornos) debería estar estrictamente controlado.

Para el código fuente, esto se puede lograr controlando el almacenamiento central de dicho código, preferiblemente en el sistema de gestión del código fuente.

El acceso de lectura y escritura al código fuente puede diferir según el rol del personal. Por ejemplo, el acceso de lectura al código fuente se puede proporcionar ampliamente dentro de la organización, pero el acceso de escritura al código fuente solo está disponible para el personal privilegiado o los propietarios designados. Cuando varios desarrolladores de una organización utilizan componentes de código, se debería implementar el acceso de lectura a un repositorio de código centralizado. Además, si se utiliza código de fuente abierta o componentes de código de terceros dentro de una organización, se puede proporcionar acceso de lectura a dichos repositorios de códigos externos. Sin embargo, el acceso de escritura aún debería estar restringido.

Se deberían considerar las siguientes pautas para controlar el acceso a las bibliotecas de fuentes de programas a fin de reducir el potencial de corrupción de los programas de computadora:

a) gestionar el acceso al código fuente del programa y las bibliotecas fuente del programa de acuerdo con los procedimientos establecidos;

b) otorgar acceso de lectura y escritura al código fuente basado en las necesidades comerciales y gestionado para abordar los riesgos de alteración o uso indebido y de acuerdo con los procedimientos establecidos;

c) actualización del código fuente y elementos asociados y concesión de acceso al código fuente de acuerdo con los procedimientos de control de cambios (véase 8.32) y realizarlo solo después de que se haya recibido la autorización apropiada;

d) no otorgar a los desarrolladores acceso directo al repositorio de código fuente, sino a través de herramientas de desarrollador que controlan las actividades y autorizaciones sobre el código fuente;

e) mantener listas de programas en un entorno seguro, donde el acceso de lectura y escritura debería administrarse y asignarse de manera adecuada;

f) mantener un registro de auditoría de todos los accesos y de todos los cambios al código fuente.

Si el código fuente del programa está destinado a ser publicado, se deberían considerar controles adicionales para garantizar su integridad (por ejemplo, firma digital).

Otra información

Si el acceso al código fuente no se controla adecuadamente, el código fuente puede modificarse o algunos datos en el entorno de desarrollo (por ejemplo, copias de datos de producción, detalles de configuración) pueden ser recuperados por personas no autorizadas.

8.5 Autenticación segura

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidades_y_acceso	#Protección

Control

Se deberían implementar tecnologías y procedimientos de autenticación seguros en función de las restricciones de acceso a la información y la política de tópico específico sobre el control de acceso.

Propósito

Para garantizar que un usuario o una entidad esté autenticado de forma segura, cuando se concede acceso a sistemas, aplicaciones y servicios.

Guía

Debería elegirse una técnica de autenticación adecuada para corroborar la identidad declarada de un usuario, software, mensajes y otras entidades.

La fuerza de la autenticación debería ser adecuada para la clasificación de la información a la que se accede. Cuando se requiera una autenticación sólida y una verificación de identidad, se deberían utilizar métodos de autenticación alternativos 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 los sistemas de información críticos (también conocida como autenticación multifactor). El uso de una combinación de múltiples factores de autenticación, como lo que sabe, lo que tiene y lo que es, reduce las posibilidades de accesos no autorizados. La autenticación multifactor se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, basadas en reglas y patrones predefinidos, como el acceso desde una ubicación inusual, desde un dispositivo inusual o en un momento inusual.

La información de autenticación biométrica debería invalidarse si alguna vez se ve comprometida. La autenticación biométrica puede no estar disponible dependiendo de las condiciones de uso (por ejemplo, humedad o envejecimiento). Para prepararse para estos problemas, la autenticación biométrica debería ir acompañada de al menos una técnica de autenticación alternativa.

El procedimiento para iniciar sesión en un sistema o aplicación debería diseñarse para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión deberían implementarse considerando lo siguiente:

a) no mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito para evitar proporcionar a un usuario no autorizado asistencia innecesaria;

b) mostrar un aviso general que advierte que solo los usuarios autorizados deberían acceder al sistema, la aplicación o el servicio;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayudarían a un usuario no autorizado (por ejemplo, si surge una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta);

d) validar la información de inicio de sesión solo al completar todos los datos de entrada;

e) protección contra intentos de inicio de sesión por fuerza bruta en nombres de usuario y contraseñas (por ejemplo, usando CAPTCHA, requiriendo el restablecimiento de contraseña después de un número predefinido de intentos fallidos o bloqueando al usuario después de un número máximo de errores);

f) registrar intentos fallidos y exitosos;

g) generar un evento de seguridad si se detecta un intento potencial o exitoso de incumplimiento de los controles de inicio de sesión (por ejemplo, enviar una alerta al usuario y a los administradores del sistema de la organización cuando se haya alcanzado un cierto número de intentos de contraseña incorrectos);

h) mostrar o enviar la siguiente información en un canal separado al completar un inicio de sesión exitoso:

   1) fecha y hora del inicio de sesión exitoso anterior;

   2) detalles de cualquier intento de inicio de sesión fallido desde el último inicio de sesión exitoso;

i) no mostrar una contraseña en texto claro cuando se ingresa; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario (por ejemplo, por razones de accesibilidad o para evitar bloquear a los usuarios debido a errores repetidos);

j) no transmitir contraseñas en texto sin cifrar a través de una red para evitar ser capturado por un programa "rastreador" de la red;

k) finalizar las sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo, como áreas públicas o externas fuera de la gestión de seguridad de la organización o en los dispositivos terminales de los usuarios;

l) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

Otra información

Se puede encontrar información adicional sobre la garantía de autenticación de entidades en ISO/IEC 29115.

8.6 Gestión de capacidad

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Continuidad	#Governanza_y_ecosistema #Protección

Control

El uso de recursos debería monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.

Propósito

Asegurar la capacidad requerida de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones.

Guía

Deberían identificarse los requisitos de capacidad para las instalaciones de procesamiento de información, los recursos humanos, las oficinas y otras instalaciones, teniendo en cuenta la importancia comercial de los sistemas y procesos en cuestión.

El ajuste y la supervisión del sistema deberían aplicarse para garantizar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de los sistemas.

La organización debería realizar pruebas de estrés de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema disponible para cumplir con los requisitos de rendimiento máximo.

Deberían establecerse controles detectivos para indicar problemas a su debido tiempo.

Las proyecciones de los requisitos de capacidad futuros deberían tener en cuenta los nuevos requisitos del negocio y del sistema y las tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización.

Se debería prestar especial atención a los recursos con plazos de adquisición prolongados o costos elevados. Por lo tanto, los gerentes, propietarios de productos o servicios deberían monitorear la utilización de los recursos clave del sistema.

Los gerentes deberían usar la información de capacidad para identificar y evitar posibles limitaciones de recursos y la dependencia del personal clave que puede representar una amenaza para la seguridad o los servicios del sistema y planificar la acción apropiada.

Se puede lograr una capacidad suficiente aumentando la capacidad o reduciendo la demanda. Se debería considerar lo siguiente para aumentar la capacidad:

a) contratación de nuevo personal;

b) obtención de nuevas instalaciones o espacio;

c) adquirir sistemas de procesamiento, memoria y almacenamiento más potentes;

d) hacer uso de la computación en la nube, que tiene características inherentes que abordan directamente los problemas de capacidad. La computación en la nube tiene elasticidad y escalabilidad que permiten una rápida expansión y reducción bajo demanda de los recursos disponibles para aplicaciones y servicios particulares.

Se debería considerar lo siguiente para reducir la demanda de los recursos de la organización:

a) eliminación de datos obsoletos (espacio en disco);

b) eliminación de registros impresos que hayan cumplido su período de retención (liberar espacio en las estanterías);

c) desmantelamiento de aplicaciones, sistemas, bases de datos o entornos;

d) optimizar los procesos y programas por lotes;

e) optimizar el código de la aplicación o las consultas a la base de datos;

f) negar o restringir el ancho de banda para los servicios que consumen recursos si estos no son críticos (por ejemplo, transmisión de video).

Se debería considerar un plan de gestión de la capacidad documentado para los sistemas de misión crítica.

Otra información

Para obtener más detalles sobre la elasticidad y escalabilidad de la conmutación en la nube, consulte ISO/IEC TS 23167.

8.7 Protección contra malware

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_en_sistemas_y_redes #Protección_de_la_información	#Protección #Defensa

Control

La protección contra el malware debería implementarse y respaldarse mediante la concienciación adecuada del usuario.

Propósito

Para garantizar que la información y otros activos asociados estén protegidos contra el malware.

Guía

La protección contra el malware debería basarse en el software de detección y reparación de malware, el conocimiento de la seguridad de la información, el acceso adecuado al sistema y los controles de gestión de cambios. El uso de software de detección y reparación de malware por sí solo no suele ser adecuado. deberían tenerse en cuenta las siguientes orientaciones:

a) implementar reglas y controles que eviten o detecten el uso de software no autorizado [por ejemplo, lista de aplicaciones permitidas (es decir, utilizando una lista que proporcione las aplicaciones permitidas)] (véanse 8.19 y 8.32);

b) implementar controles que eviten o detecten el uso de sitios web maliciosos conocidos o sospechosos (por ejemplo, listas de bloqueo);

c) reducir las vulnerabilidades que pueden ser explotadas por malware [por ejemplo, mediante la gestión de vulnerabilidades técnicas (véase 8.8 y 8.19)];

d) llevar a cabo una validación automatizada regular del software y el contenido de datos de los sistemas, especialmente para los sistemas que respaldan los procesos comerciales críticos; investigar la presencia de archivos no aprobados o enmiendas no autorizadas;

e) establecer medidas de protección frente a los riesgos asociados a la obtención de archivos y software, ya sea a través de redes externas o por cualquier otro medio;

f) instalar y actualizar regularmente software de detección y reparación de malware para escanear computadoras y medios de almacenamiento electrónico. Realizar exploraciones periódicas 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 su uso. Realizar este escaneo en diferentes lugares (por ejemplo, en servidores de correo electrónico, computadoras de escritorio) y al ingresar a la red de la organización;

3) escanear páginas web en busca de malware cuando se accede a ellas;

g) determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los resultados de la evaluación de riesgos y teniendo en cuenta:

1) defensa en profundidad de los principios donde serían más efectivos. Por ejemplo, esto puede conducir a la detección de malware en una puerta de enlace de red (en varios protocolos de aplicación, como correo electrónico, transferencia de archivos y web), así como en los dispositivos y servidores de punto final del usuario;

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) tener cuidado de protegerse contra la introducción de malware durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra el malware;

i) implementar un proceso para autorizar la desactivación temporal o permanente de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra software malintencionado interrumpe las operaciones normales;

j) preparar planes de continuidad del negocio adecuados para la recuperación de ataques de malware, incluida la copia de seguridad de todos los datos y software necesarios (incluida la copia de seguridad en línea y fuera de línea) y las medidas de recuperación (véase 8.13);

k) aislar ambientes donde pueden ocurrir consecuencias catastróficas;

l) definir procedimientos y responsabilidades para abordar la protección contra el malware en los sistemas, incluida la capacitación en su uso, la notificación y la recuperación de ataques de malware;

m) proporcionar conciencia o capacitación (véase 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 [la información recopilada en n) y o) se puede utilizar para garantizar la concientización y la formación se mantiene actualizada];

n) implementar procedimientos para recopilar información periódicamente sobre nuevos programas maliciosos, como suscribirse a listas de correo o revisar sitios web relevantes;

o) verificar que la información relacionada con el malware, como los boletines de advertencia, proviene de fuentes calificadas y acreditadas (por ejemplo, sitios de Internet confiables 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 la computadora, de modo que los controles de malware comunes no pueden limpiar el sistema y una nueva imagen completa del software del sistema operativo y, a veces, el firmware de la computadora es necesaria 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 operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #proteger	#Gestión_de_amenazas_y_vulnerabilidades	#Gobernanza_y_Ecosistema #Protección #Defensa

Control

Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debería evaluar la exposición de la organización a tales vulnerabilidades y se deberían tomar las medidas apropiadas.

Propósito

Para evitar la explotación de vulnerabilidades técnicas.

Guía

Identificación de vulnerabilidades técnicas

La organización debería tener un inventario preciso de activos (véase 5.9 a 5.14) como un requisito previo para una gestión técnica de vulnerabilidad eficaz; El inventario debería incluir el proveedor de software, el nombre del software, los números de versión, el estado actual de implementación (por ejemplo, qué software está instalado en qué sistemas) y la (s) persona (s) dentro de la organización responsable del software.

Para identificar vulnerabilidades técnicas, la organización debería considerar:

a) definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de la vulnerabilidad, incluido el seguimiento de la vulnerabilidad, la evaluación del riesgo de vulnerabilidad, la actualización, el seguimiento de los activos y las responsabilidades de coordinación necesarias;

b) para software y otras tecnologías (según la lista de inventario de activos, véase 5.9), identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener el conocimiento sobre ellas. 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 los proveedores de sistemas de información (incluidos sus componentes) que garanticen la notificación, el manejo y la divulgación de vulnerabilidades, incluidos los requisitos de los contratos aplicables (véase 5.20);

d) utilizar herramientas de escaneo de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y verificar si el parcheo de vulnerabilidades fue exitoso;

e) realizar pruebas de penetración planificadas, documentadas y repetibles o evaluaciones de vulnerabilidad por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades. Actuar con cautela ya que tales actividades pueden comprometer la seguridad del sistema;

f) seguimiento del uso de bibliotecas de terceros y código fuente en busca de vulnerabilidades. Esto debería incluirse en la codificación segura (consulte 8.28).

La organización debería desarrollar procedimientos y capacidades para:

a) detectar la existencia de vulnerabilidades en sus productos y servicios incluyendo cualquier componente externo utilizado en estos;

b) recibir informes de vulnerabilidad de fuentes internas o externas.

La organización debería proporcionar un punto de contacto público como parte de una política de tema específico sobre la divulgación de vulnerabilidades para que los investigadores y otras personas puedan informar problemas. Las organizaciones deberían establecer procedimientos de notificación de vulnerabilidades, formularios de notificación en línea y hacer uso de la inteligencia de amenazas adecuada o foros de intercambio de información. Las organizaciones también deberían considerar los programas de recompensas por errores donde las recompensas se ofrecen como un incentivo para ayudar a las organizaciones a identificar vulnerabilidades con el fin de remediarlas de manera adecuada. La organización también debería compartir información con los organismos industriales competentes u otras partes interesadas.

Evaluación de vulnerabilidades técnicas

Para evaluar las vulnerabilidades técnicas identificadas, se debería considerar la siguiente guía:

a) analizar y verificar informes para determinar qué respuesta y actividad de remediación se necesita;

b) una vez identificada una potencial vulnerabilidad técnica, identificar los riesgos asociados y las acciones a tomar. Tales acciones pueden implicar la actualización de sistemas vulnerables o la aplicación de otros controles.

Tomar las medidas adecuadas para abordar las vulnerabilidades técnicas

Se debería implementar un proceso de administración de actualizaciones de software para garantizar que se instalen los parches aprobados más actualizados y las actualizaciones de aplicaciones 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 deberían probarse y documentarse por completo, de modo que se puedan volver a aplicar, si es necesario, a futuras actualizaciones de software. Si es necesario, las modificaciones deberían ser probadas y validadas por un organismo de evaluación independiente.

Se debería considerar la siguiente guía para abordar las vulnerabilidades técnicas:

a) tomar medidas apropiadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un cronograma para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

b) dependiendo de la urgencia de abordar una vulnerabilidad técnica, llevar a cabo la acción de acuerdo con los controles relacionados con la gestión de cambios (véase 8.32) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (véase 5.26);

c) usar solo actualizaciones de fuentes legítimas (que pueden ser internas o externas a la organización);

d) probar y evaluar las actualizaciones antes de que se instalen para asegurarse de que sean efectivas y no produzcan efectos secundarios que no se puedan tolerar; [es decir, si hay una actualización disponible, evaluar los riesgos asociados con la instalación de la actualización (los riesgos que plantea la vulnerabilidad deberían compararse con el riesgo de instalar la actualización)];

e) abordar primero los sistemas de alto riesgo;

f) desarrollar soluciones (normalmente actualizaciones de software o parches);

g) prueba para confirmar si la remediación o mitigación es efectiva;

h) proporcionar mecanismos para verificar la autenticidad de la remediación;

i) si no hay actualización disponible o no se puede instalar la actualización, considerando otros controles, tales como:

   1) aplicar cualquier solución alternativa sugerida por el proveedor de software u otras fuentes relevantes;

   2) apagar servicios o capacidades relacionados con la vulnerabilidad;

   3) adaptar o agregar controles de acceso (por ejemplo, cortafuegos) en las fronteras de la red (véase 8.20 a 8.22);

   4) proteger sistemas, dispositivos o aplicaciones vulnerables de ataques mediante la implementación de filtros de tráfico adecuados (a veces denominados parches virtuales);

   5) aumento de la supervisión para detectar ataques reales;

6) sensibilización sobre la vulnerabilidad.

En el caso del software adquirido, si los proveedores publican regularmente información sobre actualizaciones de seguridad para su software y brindan la posibilidad de instalar dichas actualizaciones automáticamente, la organización debería decidir si utilizar la actualización automática o no.

Otras consideraciones

Se debería mantener un registro de auditoría de todos los pasos realizados en la gestión de vulnerabilidades técnicas. El proceso de gestión de la vulnerabilidad técnica debería supervisarse y evaluarse periódicamente para garantizar su eficacia y eficiencia.

Un proceso de gestión de vulnerabilidad técnica eficaz 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 llevarán a cabo en caso de que ocurra un incidente.

Cuando la organización utiliza un servicio en la nube proporcionado por un proveedor de servicios en la nube externo, el proveedor de servicios en la nube debería garantizar la gestión de la vulnerabilidad técnica de los recursos del proveedor de servicios en la nube. Las responsabilidades del proveedor de servicios en la nube para la gestión de vulnerabilidades técnicas deberían ser parte del contrato de servicio en la nube y esto debería incluir procesos para informar las acciones del proveedor de servicios en la nube relacionadas con las vulnerabilidades técnicas (véase 5.23). Para algunos servicios en la nube, existen responsabilidades respectivas para el proveedor de servicios en la nube y el cliente del servicio en la nube. Por ejemplo, el cliente del servicio en la nube es responsable de la gestión de vulnerabilidades de sus propios activos utilizados para los servicios en la nube.

Otra información

La gestión de vulnerabilidades técnicas puede verse como una subfunción de la gestión de cambios y, como tal, puede aprovechar los procesos y procedimientos de gestión de cambios (véase 8.32).

Existe la posibilidad de que una actualización no aborde el problema de manera adecuada y tenga efectos secundarios negativos. Además, en algunos casos, la desinstalación de una actualización no se puede lograr fácilmente una vez que se ha aplicado la actualización.

Si no es posible realizar pruebas adecuadas de las actualizaciones (por ejemplo, debido a costos o falta de recursos), se puede considerar una demora en la actualización para evaluar los riesgos asociados, en función de la experiencia informada por otros usuarios. El uso de ISO/IEC 27031 puede resultar beneficioso.

Cuando se producen parches o actualizaciones de software, la organización puede considerar la posibilidad de proporcionar un proceso de actualización automatizado en el que estas actualizaciones se instalen en los sistemas o productos afectados sin la necesidad de que el cliente o el usuario intervengan. Si se ofrece un proceso de actualización automático, puede permitir al cliente o usuario elegir una opción para desactivar la actualización automática o controlar el momento de la instalación de la actualización.

Cuando el proveedor proporciona un proceso de actualización automatizado y las actualizaciones se pueden instalar en los sistemas o productos afectados sin necesidad de intervención, la organización determina si aplica el proceso automatizado o no. Una razón para no elegir la actualización automática es mantener el control sobre cuándo se realiza la actualización. Por ejemplo, un software utilizado para una operación comercial no se puede actualizar hasta que la operación se haya completado.

Una debilidad del escaneo de vulnerabilidades es que es posible que no tenga en cuenta completamente la defensa en profundidad: dos contramedidas que siempre se invocan en secuencia pueden tener vulnerabilidades que están enmascaradas por fortalezas en la otra. La contramedida compuesta no es vulnerable, mientras que un escáner de vulnerabilidades puede informar que ambos componentes son vulnerables. Por lo tanto, las organizaciones deberían tener cuidado al revisar y actuar sobre los informes de vulnerabilidad.

Muchas organizaciones suministran software, sistemas, productos y servicios no solo dentro de la organización, sino también a las partes interesadas, como clientes, socios u otros usuarios. Estos software, sistemas, productos y servicios pueden tener vulnerabilidades de seguridad de la información que afectan la seguridad de los usuarios.

Las organizaciones pueden publicar soluciones y divulgar información sobre vulnerabilidades a los usuarios (generalmente a través de un aviso público) y proporcionar información adecuada para los servicios de bases de datos de vulnerabilidades de software.

Para obtener más información relacionada con la gestión de vulnerabilidades técnicas al utilizar la computación en la nube, consulte la serie ISO/IEC 19086 e ISO/IEC 27017.

ISO/IEC 29147 proporciona información detallada sobre la recepción de informes de vulnerabilidad y la publicación de avisos de vulnerabilidad. ISO/IEC 30111 proporciona información detallada sobre el manejo y resolución de vulnerabilidades reportadas.

8.9 Gestión de la configuración

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura	#Protección

Control

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deberían establecerse, documentarse, implementarse, monitorearse y revisarse.

Propósito

Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se 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 (incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para los sistemas recién instalados, así como para los sistemas operativos durante su vida útil.

deberían existir roles, responsabilidades y procedimientos para garantizar un control satisfactorio de todos los cambios de configuración.

Plantillas estándar

Deberían definirse plantillas estándar para la configuración segura de hardware, software, servicios y redes:

a) utilizar orientación disponible públicamente (por ejemplo, plantillas predefinidas de proveedores y de organizaciones de seguridad independientes);

b) considerar el nivel de protección necesario para determinar un nivel suficiente de seguridad;

c) respaldar la política de seguridad de la información de la organización, las políticas de temas específicos, los estándares y otros requisitos de seguridad;

d) considerar la viabilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización.

Las plantillas deberían revisarse periódicamente y actualizarse cuando sea necesario abordar nuevas amenazas o vulnerabilidades, o cuando se introduzcan nuevas versiones de software o hardware.

Se debería considerar lo siguiente para establecer plantillas estándar para la configuración segura de hardware, software, servicios y redes:

a) minimizar el número de identidades con derechos de acceso privilegiados o de nivel de administrador;

b) deshabilitar identidades innecesarias, no utilizadas o inseguras;

c) inhabilitar o restringir funciones y servicios innecesarios;

d) restringir el acceso a poderosos programas de utilidad y configuraciones de parámetros del host;

e) sincronizar relojes;

f) cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad predeterminados;

g) invocar instalaciones de tiempo de espera que desconectan automáticamente los dispositivos informáticos después de un período predeterminado de inactividad;

h) verificar que se hayan cumplido los requisitos de la licencia (véase 5.32).

Gestionar configuraciones

Las configuraciones establecidas de hardware, software, servicios y redes deberían registrarse y debería mantenerse un registro de todos los cambios de configuración. Estos registros deberían almacenarse de forma segura. Esto se puede lograr de varias formas, como bases de datos de configuración o plantillas de configuración.

Los cambios en las configuraciones deberían seguir el proceso de gestión de cambios (véase 8.32).

Los registros de configuración pueden contener según corresponda:

a) información actualizada del propietario o del punto de contacto del activo;

b) fecha del último cambio de configuración;

c) versión de la plantilla de configuración;

d) relación con configuraciones de otros activos.

Monitoreo de configuraciones

Las configuraciones deberían monitorearse con un conjunto integral de herramientas de administración del sistema (por ejemplo, utilidades de mantenimiento, soporte remoto, herramientas de administración empresarial, software de respaldo y restauración) y deberían revisarse periódicamente para verificar los ajustes de configuración, evaluar la seguridad de las contraseñas y evaluar las actividades realizadas. Las configuraciones reales se pueden comparar con las plantillas de destino definidas. Cualquier desviación debería abordarse, ya sea mediante la aplicación automática de la configuración objetivo-definida o mediante un análisis manual de la desviación seguido de acciones correctivas.

Otra información

La documentación de los sistemas a menudo registra detalles sobre la configuración tanto del hardware como del software.

El refuerzo del sistema es una parte típica de la gestión de la configuración.

La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas.

La automatización suele ser más eficaz para gestionar la configuración de seguridad (por ejemplo, utilizando la infraestructura como código).

Las plantillas de configuración y los destinos pueden ser información confidencial y, en consecuencia, deberían protegerse contra el acceso no autorizado.

8.10 Eliminación de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información	#Protección

Control

La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento debería eliminarse cuando ya no sea necesaria.

Propósito

Para evitar la exposición innecesaria de información sensible y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.

Guía

Generalidades

La información confidencial no debería conservarse por más tiempo del necesario para reducir el riesgo de divulgación no deseada.

Al eliminar información sobre sistemas, aplicaciones y servicios, se debería considerar lo siguiente:

a) seleccionar un método de eliminación (por ejemplo, sobreescritura electrónica o borrado criptográfico) de acuerdo con los requisitos del negocio y teniendo en cuenta las leyes y regulaciones pertinentes;

b) registrar los resultados de la eliminación como evidencia;

c) al utilizar proveedores de servicios de eliminación de información, obtener evidencia de la eliminación de información de ellos.

Cuando los terceros almacenan la información de la organización en su nombre, la organización debería considerar la inclusión de requisitos sobre la eliminación de información en los acuerdos con terceros para hacerla cumplir durante y después de la terminación de dichos servicios.

Métodos de eliminación

De acuerdo con la política temática específica de la organización sobre retención de datos y teniendo en cuenta la legislación y los reglamentos pertinentes, la información confidencial debería eliminarse cuando ya no sea necesaria, mediante:

a) configurar sistemas para destruir de forma segura la información cuando ya no sea necesaria (por ejemplo, después de un período definido sujeto a la política de tópico específico sobre retención de datos o por solicitud de acceso del sujeto);

b) eliminar versiones obsoletas, copias y archivos temporales dondequiera que se encuentren;

c) usar un software de eliminación seguro y aprobado para eliminar permanentemente la información para ayudar a garantizar que la información no se pueda recuperar mediante el uso de herramientas especializadas de recuperación o forenses;

d) utilizar proveedores certificados y aprobados de servicios de eliminación segura;

e) utilizar mecanismos de eliminación apropiados para el tipo de medio de almacenamiento que se está eliminando (por ejemplo, desmagnetización de unidades de disco duro y otros medios de almacenamiento magnéticos).

Cuando se utilizan servicios en la nube, la organización debería verificar si el método de eliminación proporcionado por el 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 elimine la información. Estos procesos de eliminación deberían automatizarse de acuerdo con las políticas de tópico específico, cuando estén disponibles y sean aplicables. Dependiendo de la confidencialidad de la información eliminada, los registros pueden rastrear o verificar que estos procesos de eliminación hayan sucedido.

Para evitar la exposición involuntaria de información confidencial cuando el equipo se envía de vuelta a los proveedores, la información confidencial debería protegerse eliminando los almacenamientos auxiliares (por ejemplo, unidades de disco duro) y la memoria antes de que el equipo abandone las instalaciones de la organización.

Teniendo en cuenta que la eliminación segura de algunos dispositivos (por ejemplo, teléfonos inteligentes) solo se puede lograr mediante la destrucción o el uso de las funciones integradas en estos dispositivos (por ejemplo, "restaurar la configuración de fábrica"), la organización debería elegir el método apropiado de acuerdo con la clasificación de la información manejada por tales dispositivos.

Se deberían aplicar las medidas de control descritas en 7.14 para destruir físicamente el dispositivo de almacenamiento y eliminar simultáneamente la información que contiene.

Un registro oficial de eliminación de información es útil cuando se analiza la causa de un posible evento de fuga de información.

Otra información

La información sobre la eliminación de datos del usuario en los servicios en la nube se puede encontrar en ISO/IEC 27017.

La información sobre la eliminación de IIP se puede encontrar en ISO/IEC 27555.

8.11 Enmascaramiento de datos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información	#Protección

Control

El enmascaramiento de datos debería utilizarse de acuerdo con la política de acceso específica del tema de la organización. de control y otros requisitos relacionados, específicos del tema y del negocio, teniendo en cuenta la legislación aplicable. consideración.

Propósito

Para limitar la exposición de datos confidenciales, incluida la información de identificación personal, y para cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.

Guía

Cuando la protección de datos confidenciales (por ejemplo, IIP) es una preocupación, las organizaciones deberían considerar ocultar dichos datos. datos utilizando técnicas como el enmascaramiento de datos, la seudonimización o la anonimización.

Las técnicas de seudonimización o anonimización pueden ocultar la IIP, disfrazar la verdadera identidad de los principales de la IIP u otra información confidencial, y desconecte el vínculo entre la IIP y la identidad del principal de la IIP o el enlace entre otra información sensible.

Cuando se utilicen técnicas de seudonimización o anonimización, se debería verificar que los datos hayan sido adecuadamente seudonimizados o anonimizados. La anonimización de datos debería considerar todos los elementos de la información sensible para que sea eficaz. Por ejemplo, si no se considera adecuadamente, una persona puede identificarse, aunque se anonimicen los datos que pueden identificar directamente a esa persona, por la presencia de otros datos que permitan identificar indirectamente a la persona.

Las técnicas adicionales para el enmascaramiento de datos incluyen:

a) encriptación (que requiere que los usuarios autorizados tengan una clave);

b) anular o eliminar caracteres (evitando que los usuarios no autorizados vean los mensajes completos); c) números y fechas variables;

d) sustitución (cambiar un valor por otro para ocultar datos sensibles);

e) reemplazar valores con su hash.

Se debería considerar lo siguiente al implementar técnicas de enmascaramiento de datos:

a) no otorgar a todos los usuarios acceso a todos los datos, por lo tanto, diseñar consultas y máscaras para mostrar solo los datos mínimos requeridos al usuario;

b) hay casos en los que algunos datos no deberían ser visibles para el usuario para algunos registros de un conjunto de datos; en este caso, diseñar e implementar un mecanismo de ofuscación de datos (por ejemplo, si un paciente no quiere que el personal del hospital pueda ver todos sus registros, incluso en caso de emergencia, entonces el al personal del hospital se le presentan datos parcialmente ofuscados y solo el personal puede acceder a los datos con roles específicos si contiene información útil para un tratamiento adecuado);

c) cuando los datos están ofuscados, dando al director de IIP la posibilidad de exigir que los usuarios no puedan ver si los datos están ofuscados (ofuscación de la ofuscación; esto se usa en establecimientos de salud, por ejemplo, si el paciente no desea que el personal vea esa información confidencial, como embarazos o se han ofuscado los resultados de los análisis de sangre);

d) cualquier requisito legal o reglamentario (por ejemplo, exigir el enmascaramiento de la información de las tarjetas de pago durante el procesamiento o almacenamiento).

Se debería tener en cuenta lo siguiente al utilizar el enmascaramiento de datos, la seudonimización o la anonimización:

a) nivel de fuerza del enmascaramiento de datos, seudonimización o anonimización de acuerdo con el uso de los datos procesados;

b) controles de acceso a los datos procesados;

c) acuerdos o restricciones en el uso de los datos procesados;

d) prohibir cotejar los datos procesados con otra información para identificar al principal de la IIP;

e) realizar un seguimiento del suministro y la recepción de los datos procesados

Otra información

La anonimización altera irreversiblemente la IIP de tal manera que ya no se puede identificar al principal de la IIP directa o indirectamente.

La seudonimización reemplaza la información de identificación con un alias. Conocimiento del algoritmo. (a veces denominada "información adicional") utilizada para realizar la seudonimización permite para al menos alguna forma de identificación del principal IIP. Tal “información adicional” debería, por lo tanto, mantenerse separados y protegidos.

Si bien la seudonimización es, por lo tanto, más débil que la anonimización, los conjuntos de datos seudonimizados pueden ser más útil en la investigación estadística.

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos confidenciales. Enmascaramiento de datos puede ser estático (cuando los elementos de datos están enmascarados en la base de datos original), dinámico (usando

automatización y reglas para proteger los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

Las funciones hash se pueden utilizar para anonimizar la IIP. Para evitar ataques de enumeración, siempre debería combinarse con una función de sal.

La IIP en identificadores de recursos y sus atributos [por ejemplo, nombres de archivo, localizadores uniformes de recursos (URL)] deberían evitarse o anonimizarse adecuadamente.

Controles adicionales relacionados con la protección de información de identificación personal en nubes públicas se dan en ISO/IEC 27018.

Información adicional sobre técnicas de desidentificación está disponible en ISO/IEC 20889.

8.12 Prevención de fuga de datos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad	#Proteger #Detectar	#Protección_de_la_información	#Protección #Defensa

Control

Las medidas de prevención de fuga de datos deberían aplicarse a los sistemas, redes y cualquier otro dispositivo que procesar, almacenar o transmitir información sensible.

Propósito

Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

Guía

La organización debería considerar lo siguiente para reducir el riesgo de fuga de datos:

a) identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos);

b) monitorear los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y almacenamiento portátil) dispositivos);

c) actuar para evitar que se filtre información (por ejemplo, poner en cuarentena correos electrónicos que contengan información).

Las herramientas de prevención de fuga de datos deberían utilizarse para:

a) identificar y controlar la información sensible en riesgo de divulgación no autorizada (por ejemplo, en datos en el sistema de un usuario);

b) detectar la divulgación de información confidencial (por ejemplo, cuando la información se carga en servicios en la nube de terceros o enviados por correo electrónico);

c) bloquear acciones de usuarios o transmisiones de red que expongan información confidencial (p. copia de las entradas de la 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 a 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 la configuración de herramientas existentes que permiten a los usuarios ver y manipular datos almacenados de forma remota, pero evitan copiar y pegar fuera del control de la organización.

Si se requiere la exportación de datos, se debería permitir que el propietario de los datos apruebe la exportación y retenga a los usuarios. responsable de sus actos.

La toma de capturas de pantalla o fotografías de la pantalla debería abordarse a través de los términos y condiciones de uso, capacitación y auditoría.

Cuando se realiza una copia de seguridad de los datos, se debería tener cuidado para garantizar que la información confidencial esté protegida mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen los respaldo.

También se debería considerar la prevención de fuga de datos para proteger contra las acciones de inteligencia de un adversario obtenga información confidencial o secreta (geopolítica, humana, financiera, comercial, científico o cualquier otro) que puede ser de interés para el espionaje o puede ser crítico para la comunidad. Las acciones de prevención de fuga de datos deberían estar orientadas a confundir las decisiones del adversario, por ejemplo, al reemplazar información auténtica con información falsa, ya sea como una acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de honeypots para atraer a los atacantes

Otra información

Las herramientas de prevención de fuga de datos están diseñadas para identificar datos, monitorear el uso y movimiento de datos, y tomar medidas para evitar la fuga de datos (por ejemplo, alertar a los usuarios sobre su comportamiento de riesgo y bloquear la transferencia de datos a dispositivos portátiles de almacenamiento).

La prevención de la fuga de datos involucra inherentemente monitorear las comunicaciones del personal y en línea. actividades y, por extensión, mensajes de partes externas, lo que plantea preocupaciones legales que deberían ser considerado antes de implementar herramientas de prevención de fuga de datos. Existe una variedad de leyes relacionadas con privacidad, protección de datos, empleo, interceptación de datos y telecomunicaciones que sea aplicable a monitoreo y procesamiento de datos en el contexto de la prevención de fugas de datos.

La prevención de fuga de datos se puede respaldar con controles de seguridad estándar, como políticas específicas de temas. sobre control de acceso y gestión segura de documentos (véase 5.12 y 5.15)

8.13 Respaldo de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Protección

Control

Las copias de seguridad de la información, el software y los sistemas deberían mantenerse y probarse regularmente en de acuerdo con la política de tópico específico acordada sobre copias de seguridad.

Propósito

Para permitir la recuperación de la pérdida de datos o sistemas.

Guía

Se debería establecer una política de respaldo específica del tema para abordar la retención de datos de la organización y requisitos de seguridad de la información.

Se deberían proporcionar instalaciones de respaldo adecuadas para garantizar que toda la información y el software esenciales puedan recuperarse después de un incidente o falla o pérdida de medios de almacenamiento.

Se deberían desarrollar e implementar planes sobre cómo la organización respaldará la información, software y sistemas, para abordar la política de tópico específico sobre copias de seguridad.

Al diseñar un plan de respaldo, se deberían tener en cuenta los siguientes elementos:

a) producir registros precisos y completos de las copias de seguridad y restauración documentada procedimientos;

b) reflejar los requisitos del negocio de la organización (por ejemplo, el objetivo del punto de recuperación, véase 5.30), los requisitos de seguridad de la información involucrada y la criticidad de la información a la operación continua de la organización en la medida (por ejemplo, respaldo completo o diferencial) y frecuencia de las copias de seguridad;

c) almacenar las copias de seguridad en un lugar remoto seguro y protegido, a una distancia suficiente para escapar de cualquier daño por un desastre en el sitio principal;

d) dar a la información de respaldo un nivel adecuado de protección física y ambiental (véase capítulo 7 y 8.1) consistente con los estándares aplicados en el sitio principal;

e) probar regularmente los medios de respaldo para garantizar que se pueda confiar en ellos para uso de emergencia cuando necesario. Probar la capacidad de restaurar datos respaldados en un sistema de prueba, sin sobrescribir el medio de almacenamiento originales en caso de que el proceso de copia de seguridad o restauración falle y cause irreparables daños o pérdida;

f) proteger las copias de seguridad mediante encriptación de acuerdo con los riesgos identificados (por ejemplo, en situaciones donde la confidencialidad es de importancia);

g) asegurarse de que se detecte la pérdida inadvertida de datos antes de realizar la copia de seguridad.

Los procedimientos operativos deberían monitorear la ejecución de las copias de seguridad y abordar las fallas de los programas programados. copias de seguridad para garantizar la integridad de las copias de seguridad de acuerdo con la política de tópico específico sobre las copias de seguridad.

Las medidas de respaldo para sistemas y servicios individuales deberían probarse periódicamente para garantizar que cumplir con los objetivos de respuesta a incidentes y planes de continuidad del negocio (véase 5.30). Esto debería ser combinado con una prueba de los procedimientos de restauración y comparado con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de sistemas y servicios críticos, las medidas de respaldo deberían cubrir todos los sistemas de información, aplicaciones y datos necesarios para recuperar el sistema completo en el evento de un desastre.

Cuando la organización utiliza un servicio en la nube, las copias de seguridad de la información de la organización, Se deberían tomar aplicaciones y sistemas en el entorno de servicios en la nube. La organización debería determinar si se cumplen los requisitos de copia de seguridad y cómo se cumplen cuando se utiliza el servicio de copia de seguridad de la información proporcionada como parte del servicio en la nube.

debería determinarse el período de retención de la información comercial esencial, teniendo en cuenta cualquier requisito para la retención de copias de archivo. La organización debería considerar la eliminación de información (consulte 8.10) en medios de almacenamiento utilizados para la copia de seguridad una vez que expire el período de retención de la información y debería tener en cuenta la legislación y los reglamentos.

Otra información

Para obtener más información sobre la seguridad del almacenamiento, incluida la consideración de retención, consulte ISO/IEC 27040.

8.14 Redundancia de las instalaciones de procesamiento de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Disponibilidad	#Proteger	#Continuidad #Gestión_de_activos	#Protección #Resiliencia

Control

Las instalaciones de procesamiento de información deberían implementarse con suficiente redundancia para cumplir con la disponibilidad requisitos

Propósito

Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.

Guía

La organización debería identificar los requisitos para la disponibilidad de los servicios de negocio y la información. sistemas La organización debería diseñar e implementar la arquitectura de sistemas con la redundancia para cumplir con estos requisitos.

La redundancia se puede introducir mediante la duplicación de instalaciones de procesamiento de información en parte o en su en su totalidad (es decir, componentes de repuesto o tener dos de todo). La organización debería planificar e implementar procedimientos para la activación de los componentes redundantes y las instalaciones de procesamiento. Los procedimientos deberían establecer si los componentes redundantes y las actividades de procesamiento son siempre activada, o en caso de emergencia, automática o manualmente. Los componentes redundantes y las instalaciones de procesamiento de información deberían garantizar el mismo nivel de seguridad que las primarias.

Deberían existir mecanismos para alertar a la organización sobre cualquier falla en el procesamiento de la información. instalaciones, permitir la ejecución del procedimiento planificado y permitir la disponibilidad continua mientras las instalaciones de procesamiento de información son reparadas o reemplazadas.

La organización debería considerar lo siguiente al implementar sistemas redundantes:

a) contratación con dos o más proveedores de redes e instalaciones de procesamiento de información crítica como proveedores de servicios de Internet;

b) usar redes redundantes;

c) utilizar dos centros de datos separados geográficamente con sistemas duplicados;

d) utilizar fuentes o fuentes de alimentación físicamente redundantes;

e) usar múltiples instancias paralelas de componentes de software, con equilibrio de carga automático entre ellos (entre instancias en el mismo centro de datos o en diferentes centros de datos);

f) tener componentes duplicados en sistemas (por ejemplo, CPU, discos duros, memorias) o en redes (por ejemplo, cortafuegos, enrutadores, conmutadores).

Cuando corresponda, preferiblemente en modo de producción, los sistemas de información redundantes deberían probarse para asegúrese de que la conmutación por error de un componente a otro funcione según lo previsto.

Otra información

Existe una fuerte relación entre la redundancia y la preparación de las TIC para la continuidad del negocio (véase 5.30) especialmente si se requieren tiempos de recuperación cortos. Muchas de las medidas de despido pueden ser parte de la Estrategias y soluciones de continuidad TIC.

La implementación de redundancias puede introducir riesgos a la integridad (por ejemplo, procesos de copia datos a componentes duplicados puede introducir errores) o confidencialidad (por ejemplo, control de seguridad débil de los componentes duplicados pueden comprometer) la información y los sistemas de información, que necesitan a tener en cuenta en el diseño de sistemas de información.

La redundancia en las instalaciones de procesamiento de información generalmente no aborda la indisponibilidad de la aplicación debido a fallas dentro de una aplicación.

Con el uso de la computación en la nube pública, es posible tener múltiples versiones de información en vivo instalaciones de procesamiento, existentes en múltiples ubicaciones físicas separadas con conmutación automática por error y carga equilibrio entre ellos.

Algunas de las tecnologías y técnicas para proporcionar redundancia y conmutación por error automática en el contexto de los servicios en la nube se analiza en ISO/IEC TS 23167.

8.15 Logueo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Protección #Defensa

Control

Se deberían producir, almacenar y almacenar logs que registren actividades, excepciones, fallas y otros eventos protegido y analizado.

Propósito

Para registrar eventos, generar evidencia, asegurar la integridad de la información de registro, prevenir contra acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a una seguridad de la información incidente y para apoyar las investigaciones.

Guía

Generalidades

La organización debería determinar el propósito para el cual se crean los registros, qué datos se recopilan y registrado y cualquier requisito específico del registro para proteger y manejar los datos de registro. Esto debería ser documentado en una política de tópico específico sobre el registro.

Los registros de eventos deberían incluir para cada evento, según corresponda:

a) identificaciones de usuario;

b) actividades del Sistema

c) fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión);

d) identidad del dispositivo, identificador del sistema y ubicación;

e) direcciones de red y protocolos.

Los siguientes eventos deberían ser considerados para el registro:

a) intentos de acceso al sistema exitosos y rechazados;

b) datos exitosos y rechazados y otros intentos de acceso a recursos;

c) cambios en la configuración del sistema;

d) uso de privilegios; e) uso de programas de utilidad y aplicaciones;

f) los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;

g) alarmas emitidas por el sistema de control de acceso;

h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y detección de intrusos sistemas;

i) creación, modificación o supresión de identidades;

j) transacciones ejecutadas por los usuarios en las aplicaciones.

En algunos casos, las aplicaciones son un servicio o producto proporcionado o administrado por un tercero. Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas (véase 8.17) ya que esto permite la correlación de logs entre sistemas para análisis, alerta e investigación de un incidente.

Protección de Logs

Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no deberían tener permiso para eliminar o desactivar registros de sus propias actividades. Potencialmente pueden manipular los registros en el procesamiento de la información. instalaciones bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener responsabilidad de los usuarios privilegiados.

Los controles deberían apuntar a proteger contra cambios no autorizados en la información de registro y problemas con la instalación de registro, incluidos:

a) alteraciones en los tipos de mensajes que se registran;

b) archivos de registro que se están editando o eliminando;

c) falla en el registro de eventos o sobreescritura de eventos pasados registrados si el medio de almacenamiento mantiene un registro se excede el archivo.

Para la protección de los registros, se debería considerar el uso de las siguientes técnicas: hashing criptográfico, grabación en un archivo de solo anexar y de solo lectura, grabación en un archivo de transparencia pública.

Es posible que se requiera archivar algunos registros de auditoría debido a los requisitos de retención de datos o requisitos para recolectar y conservar evidencia (véase 5.28)

Cuando la organización necesita enviar registros del sistema o de la aplicación a un proveedor para ayudar con la depuración o errores de solución de problemas, los registros deberían ser anonimizados cuando sea posible utilizando técnicas de enmascaramiento de datos (consulte 8.11) para obtener información como nombres de usuario, direcciones IP, nombres de host o nombre de la organización, antes envío al vendedor.

Los registros de eventos pueden contener datos confidenciales e información de identificación personal. Privacidad apropiada se deberían tomar medidas de protección (véase 5.34).

Análisis de Logs

El análisis de registros debería cubrir el análisis y la interpretación de los eventos de seguridad de la información, para ayudar a identificar actividad inusual o comportamiento anómalo, que pueden representar indicadores de compromiso. El análisis de los eventos debería realizarse teniendo en cuenta:

a) las habilidades necesarias para los expertos que realizan el análisis;

b) determinar el procedimiento de análisis de registros;

c) los atributos requeridos de cada evento relacionado con la seguridad;

d) excepciones identificadas mediante el uso de reglas predeterminadas (por ejemplo, SIEM o reglas de firewall e IDS o firmas de malware);

e) patrones de comportamiento conocidos y tráfico de red estándar en comparación con actividad anómala y comportamiento (UEBA);

f) resultados de análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de big data y herramientas de análisis especializadas);

g) inteligencia de amenazas disponible.

El análisis de registros debería estar respaldado por actividades de monitoreo específicas para ayudar a identificar y analizar Comportamiento anómalo, que incluye:

a) revisar intentos exitosos y fallidos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y archivos compartidos);

b) verificar los registros de DNS para identificar conexiones de red salientes a servidores maliciosos, como los asociados con servidores de comando y control de botnet;

c) examinar los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicios) en busca de actividad dentro de sistemas y redes (por ejemplo, mediante la revisión de patrones de actividad);

d) incluir registros de eventos de monitoreo físico como entrada y salida para garantizar una mayor precisión detección y análisis de incidentes;

e) correlación de registros para permitir un análisis eficiente y altamente preciso.

Deberían identificarse los incidentes de seguridad de la información supuestos y reales (por ejemplo, infección de malware o sondeo de cortafuegos) y estar sujetos a una mayor investigación (por ejemplo, como parte de una seguridad de la información proceso de gestión de incidentes, véase 5.25.

Otra información

Los registros del sistema suelen contener un gran volumen de información, gran parte de la cual es ajena a la información. monitoreo de seguridad Para ayudar a identificar eventos significativos con fines de monitoreo de la seguridad de la información, se puede considerar el uso de programas de utilidad adecuados o herramientas de auditoría para realizar la interrogación de archivos.

El registro de eventos sienta las bases para los sistemas de monitoreo automatizados (véase 8.16) que son capaces de generando reportes consolidados y alertas sobre la seguridad del sistema.

Se puede utilizar una herramienta de gestión de eventos e información de seguridad (SIEM) o un servicio equivalente para almacenar, correlacionar, normalizar y analizar la información de registro, y generar alertas. Los SIEM tienden a requerir una cuidadosa configuración para optimizar sus prestaciones. Las configuraciones por considerar incluyen identificación y selección de fuentes de registro apropiadas, ajuste y prueba de reglas y desarrollo de casos de uso.

Los archivos de transparencia pública para el registro de registros se utilizan, por ejemplo, en la transparencia de certificados. sistemas Dichos archivos pueden proporcionar un mecanismo de detección adicional útil para protegerse contra registros manipulación.

En entornos de nube, las responsabilidades de administración de registros se pueden compartir entre el servicio de nube cliente y el proveedor de servicios en la nube. Las responsabilidades varían según el tipo de servicio en la nube siendo utilizado. Puede encontrar más orientación en ISO/IEC 27017.

8.16 Monitoreo de actividades

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Las redes, los sistemas y las aplicaciones deberían monitorearse para detectar comportamientos anómalos y acciones tomadas para evaluar posibles incidentes de seguridad de la información.

Propósito

Para detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

Guía

El alcance y el nivel de monitoreo deberían determinarse de acuerdo con el negocio y la información. requisitos de seguridad y teniendo en cuenta las leyes y reglamentos pertinentes. Registros de seguimiento deberían mantenerse durante períodos de retención definidos. Lo siguiente debería ser considerado para su inclusión dentro del sistema de monitoreo:

a) tráfico de red, sistema y aplicación entrante y saliente;

b) acceso a sistemas, servidores, equipos de red, sistema de monitoreo, aplicaciones críticas, entre otros.

c) archivos de configuración de red y sistema de nivel crítico o administrativo;

d) registros de herramientas de seguridad [p. antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fuga de datos];

e) registros de eventos relacionados con la actividad del sistema y de la red;

f) comprobar que el código que se está ejecutando está autorizado para ejecutarse en el sistema y que no ha sido manipulado (por ejemplo, mediante la recompilación para agregar código adicional no deseado);

g) uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

La organización debería establecer una línea de base de comportamiento normal y monitorear contra esta línea de base para anomalías Al establecer una línea de base, se debería considerar lo siguiente:

a) revisar la utilización de los sistemas en períodos normales y pico;

b) hora habitual de acceso, lugar de acceso, frecuencia de acceso para cada usuario o grupo de usuarios.

El sistema de monitoreo debería configurarse contra la línea de base establecida para identificar anomalías comportamiento, tales como:

a) terminación no planificada de procesos o aplicaciones;

b) actividad típicamente asociada con malware o tráfico que se origina en direcciones IP maliciosas conocidas o dominios de red (por ejemplo, aquellos asociados con servidores de comando y control de botnet);

c) características de ataque conocidas (por ejemplo, denegación de servicio y desbordamiento de búfer);

d) comportamiento inusual del sistema (por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar);

e) cuellos de botella y sobrecargas (por ejemplo, colas de la red, niveles de latencia y fluctuaciones de la red);

f) acceso no autorizado (real o intentado) a sistemas o información;

g) escaneo no autorizado de aplicaciones comerciales, sistemas y redes;

h) intentos exitosos y fallidos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y sistemas de archivos);

i) comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado.

Se debería utilizar un monitoreo continuo a través de una herramienta de monitoreo. El monitoreo debería hacerse en tiempo real o en intervalos periódicos, sujeto a las necesidades y capacidades de la organización. Las herramientas de monitoreo deberían incluir la capacidad de manejar grandes cantidades de datos, adaptarse a un panorama de amenazas en constante cambio y permitir para notificaciones en tiempo real. Las herramientas también deberían poder reconocer firmas y datos específicos o patrones de comportamiento de la red o de la aplicación. El software de monitoreo automatizado debería configurarse para generar alertas (por ejemplo, a través de consolas de administración, mensajes de correo electrónico o sistemas de mensajería instantánea) basados en umbrales predefinidos. El sistema de alerta debería ajustarse y capacitarse en la base de referencia de la organización para minimizar los falsos positivos. El personal debería estar dedicado a responder a las alertas y debería estar debidamente capacitado para interpretar con precisión posibles incidentes debería haber sistemas y procesos redundantes para recibir y responder a las alertas notificaciones.

Los eventos anormales deberían ser comunicados a las partes relevantes para mejorar las siguientes actividades: auditoría, evaluación de seguridad, exploración y monitoreo de vulnerabilidades (véase 5.25). Procedimientos debería existir para responder a los indicadores positivos del sistema de monitoreo de manera oportuna, en para minimizar el efecto de los eventos adversos (véase 5.26) en la seguridad de la información. Los procedimientos deberían también se establecerá para identificar y abordar los falsos positivos, incluido el ajuste del software de monitoreo para reducir el número de futuros falsos positivos.

Otra información

El monitoreo de la seguridad se puede mejorar mediante:

a) aprovechar los sistemas de inteligencia de amenazas (véase 5.7);

b) aprovechar las capacidades de aprendizaje automático e inteligencia artificial;

c) usar listas de bloqueo o listas de permitidos;

d) realizar una variedad de evaluaciones de seguridad técnica (por ejemplo, evaluaciones de vulnerabilidad, penetración pruebas, simulaciones de ataques cibernéticos y ejercicios de respuesta cibernética), y utilizando los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable;

e) utilizar sistemas de seguimiento del rendimiento para ayudar a establecer y detectar comportamientos anómalos;

f) aprovechamiento de registros en combinación con sistemas de seguimiento.

Las actividades de monitoreo a menudo se llevan a cabo utilizando software especializado, como la detección de intrusos en sistemas. Estos se pueden configurar a una línea base de sistema y red normales, aceptables y esperados.

El monitoreo de comunicaciones anómalas ayuda en la identificación de botnets (es decir, un conjunto de dispositivos bajo el control malicioso del propietario de la botnet, generalmente utilizada para montar denegación de servicio distribuida ataques a otros equipos de otras organizaciones). Si la computadora está siendo controlada por un dispositivo, existe una comunicación entre el dispositivo infectado y el controlador. La organización, por lo tanto, deberían emplear tecnologías para monitorear comunicaciones anómalas y tomar tal acción según sea necesario.

8.17 Sincronización de reloj

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Detectivo	#Integridad	#Proteger #Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Protección #Defensa

Control

Los relojes de los sistemas de procesamiento de información utilizados por la organización deberían sincronizarse para fuentes de tiempo aprobadas.

Propósito

Para permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y para Apoyar las investigaciones sobre incidentes de seguridad de la información.

Guía

Requisitos externos e internos para la representación del tiempo, sincronización confiable y precisión debería ser documentado e implementado. Dichos requisitos pueden ser de carácter legal, estatutario, reglamentario, necesidades contractuales, normativas y de control interno. Un tiempo de referencia estándar para uso dentro del La organización debería definirse y considerarse para todos los sistemas, incluidos los sistemas de gestión de edificios, sistemas de entrada y salida y otros que puedan ser utilizados 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) debería utilizarse como reloj de referencia para los sistemas de registro; una fuente consistente y confiable de fecha y hora para garantizar sellos de tiempo precisos. Protocolos como el protocolo de tiempo de red (PTR) o el protocolo de tiempo de precisión (PTP) debería utilizarse para mantener todos los sistemas en red sincronizados con un reloj de referencia.

La organización puede usar dos fuentes de tiempo externas al mismo tiempo para mejorar la confiabilidad de relojes externos, y gestionar adecuadamente cualquier variación.

La sincronización del reloj puede ser difícil cuando se usan múltiples servicios en la nube o cuando se usan ambas nubes. y servicios en las instalaciones. En este caso, se debería monitorear el reloj de cada servicio y la diferencia registrados para mitigar los riesgos derivados de las discrepancias.

Otra información

La configuración correcta de los relojes de la computadora es importante para garantizar la precisión de los registros de eventos, que pueden ser requerida para investigaciones o como evidencia en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar tales investigaciones y dañar la credibilidad de tales evidencias.

8.18 Uso de programas de utilidad privilegiados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_sistemas_y_redes #Configuración_segura #Seguridad_en_aplicaciones	#Protección

Control

Se debería evitar el uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones. restringida y estrictamente controlada.

Propósito

Para garantizar que el uso de programas de utilidad no dañe el sistema y los controles de aplicaciones para la información seguridad.

Guía

Las siguientes pautas para el uso de programas de utilidad que pueden anular el sistema y los controles de aplicación deberían ser considerados:

a) limitación del uso de programas de utilidad al número mínimo práctico de confiables, autorizados usuarios (véase 8.2);

b) uso de procedimientos de identificación, autenticación y autorización para programas de utilidad, incluyendo identificación única de la persona que utiliza el programa de utilidad;

c) definición y documentación de niveles de autorización para programas de servicios;

d) autorización para uso ad hoc de programas utilitarios;

e) no poner programas de utilidad a disposición de los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere segregación de funciones;

f) eliminar o deshabilitar todos los programas de utilidad innecesarios;

g) como mínimo, separación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, segregar las comunicaciones de red para dichos programas del tráfico de aplicaciones;

h) limitación de la disponibilidad de los programas de utilidad (por ejemplo, durante la duración de un cambio autorizado);

i) registro de todos los usos de los programas de utilidad.

Otra información

La mayoría de los sistemas de información tienen uno o más programas de utilidad que pueden anular el sistema. y controles de aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, herramientas de copia de seguridad y red.

8.19 Instalación de software en sistemas operacionales

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura #Seguridad_en_las_aplicaciones	#protección

Control

Deberían implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos.

Propósito

Para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.

Guía

Se deberían considerar las siguientes pautas para administrar de forma segura los cambios y la instalación del software sobre sistemas operativos:

a) realizar actualizaciones del software operativo solo por parte de administradores capacitados según corresponda autorización de gestión (véase 8.5);

b) asegurarse de que solo se instale código ejecutable aprobado y no código de desarrollo o compiladores en sistemas operativos;

c) solo instalar y actualizar el software después de pruebas extensas y exitosas (véase 8.29 y 8.31);

d) actualizar todas las bibliotecas fuente de programas correspondientes;

e) usar un sistema de control de configuración para mantener el control de todo el software operativo, así como la documentación del sistema;

f) definir una estrategia de reversión antes de que se implementen los cambios;

g) mantener un registro de auditoría de todas las actualizaciones del software operativo;

h) archivar versiones antiguas de software, junto con toda la información y los parámetros requeridos, procedimientos, detalles de configuración y software de soporte como medida de contingencia, y para siempre que el software sea necesario para leer o procesar datos archivados.

Cualquier decisión de actualizar a una nueva versión debería tener en cuenta los requisitos del negocio para el cambio y la seguridad de la publicación (por ejemplo, la introducción de una nueva funcionalidad de seguridad de la información o el número y la gravedad de las vulnerabilidades de seguridad de la información que afectan a la versión actual). Software los parches deberían aplicarse cuando pueden ayudar a eliminar o reducir las vulnerabilidades de seguridad de la información (véase 8.8 y 8.19).

El software de computadora puede basarse en software y paquetes suministrados externamente (por ejemplo, programas de software usando módulos que están alojados en sitios externos), que deberían ser monitoreados y controlados para evitar cambios no autorizados, ya que pueden introducir vulnerabilidades de seguridad de la información.

El software suministrado por el proveedor que se utiliza en los sistemas operativos debería mantenerse en un nivel compatible por el proveedor. Con el tiempo, los proveedores de software dejarán de admitir versiones anteriores de software. La organización debería considerar los riesgos de depender de software sin soporte. Software de código abierto utilizado en los sistemas operativos debería mantenerse a la última versión adecuada del software. Sobre tiempo, el código fuente abierto puede dejar de mantenerse, pero todavía está disponible en un software de código abierto repositorio.

La organización también debería considerar los riesgos de confiar en código abierto sin mantenimiento. software cuando se utiliza en sistemas operativos. Cuando los proveedores participan en la instalación o actualización de software, el acceso físico o lógico debería sólo se dará cuando sea necesario y con la debida autorización. Las actividades del proveedor deberían ser monitoreado (véase 5.22).

La organización debería definir y hacer cumplir reglas estrictas sobre qué tipos de software pueden instalar los usuarios.

El principio de privilegio mínimo debería aplicarse 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 el 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 deberían otorgarse en función de las funciones de los usuarios en cuestión.

Otra información

No hay otra información.

8.20 Seguridad de redes

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #detectar	#Seguridad_en_sistemas_y_redes	#protección

Control

Las redes y los dispositivos de red deberían protegerse, administrarse y controlarse para proteger la información en sistemas y aplicaciones.

Propósito

Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo de compromiso a través de la red.

Guía

Deberían implementarse controles para garantizar la seguridad de la información en las redes y para proteger servicios conectados del acceso no autorizado. En particular, se deberían considerar los siguientes elementos:

a) el tipo y nivel de clasificación de la información que la red puede soportar;

b) establecer responsabilidades y procedimientos para la gestión de equipos de red y dispositivos;

c) mantener actualizada la documentación, incluidos los diagramas de red y los archivos de configuración de dispositivos (por ejemplo, enrutadores, conmutadores);

d) separar la responsabilidad operativa de las redes de las operaciones del sistema TIC cuando corresponda (véase 5.3);

e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan al público redes, redes de terceros o a través de redes inalámbricas y para proteger los sistemas conectados y aplicaciones (véase 5.22, 8.24, 5.14 y 6.6). También se pueden requerir controles adicionales para mantener la disponibilidad de los servicios de red y las computadoras conectadas a la red;

f) registro y seguimiento adecuados para permitir el registro y la detección de acciones que pueden afectar, o son relevantes para la seguridad de la información (véase 8.16 y 8.15);

g) coordinar estrechamente las actividades de gestión de la red para optimizar el servicio de la organización y para asegurar que los controles se aplican de manera consistente en todo el proceso de información infraestructura;

h) sistemas de autenticación en la red;

i) restringir y filtrar la conexión de los sistemas a la red (por ejemplo, usando firewalls);

j) detectar, restringir y autenticar la conexión de equipos y dispositivos a la red;

k) endurecimiento de los dispositivos de red;

l) segregar los canales de administración de red de otro tráfico de red;

m) aislar temporalmente subredes críticas (por ejemplo, con puentes levadizos) si la red está bajo ataque;

n) deshabilitar protocolos de red vulnerables.

La organización debería asegurarse de que se apliquen los controles de seguridad apropiados al uso de sistemas virtualizados. redes Las redes virtualizadas también cubren las redes definidas por software (SDN, SD-WAN). virtualizado redes pueden ser deseables desde el punto de vista de la seguridad, ya que pueden permitir la separación lógica de comunicación que tiene lugar a través de redes físicas, particularmente para sistemas y aplicaciones que son implementado usando computación distribuida.

Otra información

Puede encontrar información adicional sobre la seguridad de la red en la serie ISO/IEC 27033. Se puede encontrar más información sobre redes virtualizadas en ISO/IEC TS 23167.

8.21 Seguridad de servicios de red

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_sistemas_y_redes	#protección

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deberían identificarse, implementarse y monitorearse.

Propósito

Para garantizar la seguridad en el uso de los servicios de red.

Guía

Las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de servicio, deberían ser identificadas e implementadas (por proveedores de servicios de red internos o externos). La organización debería asegurarse de que los proveedores de servicios de red implementen estas medidas.

La capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura debería determinarse y controlarse periódicamente. El derecho a la auditoría debería acordarse entre la organización y el proveedor. La organización también debería considerar las certificaciones de terceros proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Las reglas sobre el uso de redes y servicios de red deberían formularse e implementarse para cubrir:

a) las redes y los servicios de red a los que se permite acceder;

b) requisitos de autenticación para acceder a diversos servicios de red;

c) procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red;

d) administración de redes y controles tecnológicos y procedimientos para proteger el acceso a conexiones de red y servicios de red;

e) los medios utilizados para acceder a las redes y servicios de red [p. uso de red privada virtual (VPN) o red inalámbrica];

f) hora, ubicación y otros atributos del usuario al momento del acceso;

g) seguimiento del uso de los servicios de red.

Se deberían considerar las siguientes características de seguridad de los servicios de red:

a) tecnología aplicada para la seguridad de los servicios de red, como autenticación, encriptación y controles de conexión a la red;

b) parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión a la red;

c) almacenamiento en caché (por ejemplo, en una red de entrega de contenido) y sus parámetros que permiten a los usuarios elegir el uso del almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad;

d) procedimientos para el uso de servicios de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.

Otra información

Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administrada, como firewalls y sistemas de detección de intrusos. Estos servicios pueden variar desde ancho de banda simple no administrado hasta ofertas complejas de valor agregado.

En ISO/IEC 29146 se proporciona más orientación sobre un marco para la gestión de acceso.

8.22 Segregación de redes

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_sistemas_y_redes	#protección

Control

Los grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en las redes de la organización.

Propósito

Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales.

Guía

La organización debería considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet). Los dominios se pueden elegir en función de los niveles de confianza, criticidad y sensibilidad (por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de alto y bajo riesgo), junto con unidades organizativas (por ejemplo, recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio de servidor que se conecta a varias unidades organizativas). La segregación se puede realizar usando redes físicamente diferentes o usando diferentes redes lógicas.

El perímetro de cada dominio debería estar bien definido. Si se permite el acceso entre dominios de red, debería controlarse en el perímetro mediante una puerta de enlace (por ejemplo, un cortafuegos, un enrutador de filtrado). Los criterios para la segregación de redes en dominios y el acceso permitido a través de las puertas de enlace deberían basarse en una evaluación de los requisitos de seguridad de cada dominio. La evaluación debería estar de

acuerdo con la política de tópico específico sobre control de acceso (véase 5.15), requisitos de acceso, valor y clasificación de la información procesada y tener en cuenta el costo relativo y el impacto en el rendimiento de incorporar tecnología de puerta de enlace adecuada.

Las redes inalámbricas requieren un tratamiento especial debido al perímetro de red mal definido. Se debería considerar el ajuste del excedente de radio para la segregación de redes inalámbricas. Para entornos sensibles, se debería considerar tratar todos los accesos inalámbricos como conexiones externas y segregar este acceso de las redes internas hasta que el acceso haya pasado a través de una puerta de enlace de acuerdo con los controles de la red (véase 8.20) antes de otorgar acceso a los sistemas internos. La red de acceso inalámbrico para invitados debería separarse de las del personal si el personal solo usa dispositivos de punto final de usuario controlados que cumplen con las políticas específicas del tema de la organización. El WiFi para invitados debería tener al menos las mismas restricciones que el WiFi para el personal, a fin de desalentar el uso del WiFi de invitados por parte del personal.

Otra información

Las redes a menudo se extienden más allá de los límites organizacionales, ya que se forman asociaciones comerciales que requieren la interconexión o el intercambio de instalaciones de redes y procesamiento de información. Dichas extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que usan la red, algunos de los cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.

8.23 Filtrado web

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_sistemas_y_redes	#protección

Control

El acceso a sitios web externos debería administrarse para reducir la exposición a contenido malicioso.

Propósito

Para proteger los sistemas contra el malware y evitar el acceso a recursos web no autorizados.

Guía

La organización debería reducir los riesgos de que su personal acceda a sitios web que contengan información ilegal o que se sepa que contienen virus o material de phishing. Una técnica para lograr esto funciona bloqueando la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware hacen esto automáticamente o pueden configurarse para hacerlo.

La organización debería identificar los tipos de sitios web a los que el personal debería o no tener acceso. La organización debería considerar bloquear el acceso a los siguientes tipos de sitios web:

a) sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas;

b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing);

c) servidores de mando y control;

d) sitio web malicioso adquirido de inteligencia de amenazas (véase 5.7);

e) sitios web que comparten contenido ilegal.

Antes de implementar este control, la organización debería establecer reglas para el uso seguro y apropiado de los recursos en línea, incluida cualquier restricción a sitios web y

aplicaciones basadas en la web indeseables o inapropiados. Las reglas deberían mantenerse actualizadas.

Se debería brindar capacitación al personal sobre el uso seguro y apropiado de los recursos en línea, incluido el acceso a la web. La capacitación debería incluir las reglas de la organización, el punto de contacto para plantear problemas de seguridad y el proceso de excepción cuando se necesita acceder a recursos web restringidos por razones comerciales legítimas. También se debería capacitar al personal para asegurarse de que no invalide ningún aviso del navegador que informe que un sitio web no es seguro, pero permite que el usuario continúe.

Otra información

El filtrado web puede incluir una variedad de técnicas que incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a evitar que el software y otras actividades maliciosas ataquen la red y los sistemas de la organización.

8.24 Uso de criptografía

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_ segura	#protección

Control

Deberían definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

Propósito

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos del negocio y de seguridad de la información, y teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

Guía

Generalidades

Al usar criptografía, se debería considerar lo siguiente:

a) la política de tópico específico sobre criptografía definida por la organización, incluidos los principios generales para la protección de la información. Es necesaria una política específica sobre el uso de la criptografía para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y para evitar el uso inapropiado o incorrecto;

b) identificar el nivel de protección requerido y la clasificación de la información y en consecuencia establecer el tipo, fortaleza y calidad de los algoritmos criptográficos requeridos;

c) el uso de criptografía para la protección de la información contenida en los dispositivos móviles o medios de almacenamiento de los usuarios y transmitida a través de redes a dichos dispositivos o medios de almacenamiento;

d) el enfoque de la gestión de claves, incluidos los métodos para gestionar la generación y protección de claves criptográficas y la recuperación de información cifrada en caso de pérdida, compromiso o daño de claves;

e) roles y responsabilidades para:

1) la implementación de las reglas para el uso efectivo de la criptografía;

2) la gestión de claves, incluida la generación de claves (véase 8.24);

f) los estándares a adoptar, así como los algoritmos criptográficos, la fuerza del cifrado, las soluciones criptográficas y las prácticas de uso que se aprueban o requieren para su uso en la organización;

g) el impacto del uso de información cifrada en los controles que se basan en la inspección de contenido (por ejemplo, detección de malware o filtrado de contenido).

Al implementar las reglas de la organización para el uso eficaz de la criptografía, se deberían tener en cuenta las reglamentaciones y las restricciones nacionales que pueden aplicarse al uso de técnicas criptográficas en diferentes partes del mundo, así como los problemas del flujo transfronterizo de información cifrada (véase 5.31).

El contenido de los acuerdos o contratos de nivel de servicio con proveedores externos de servicios criptográficos (por ejemplo, con una autoridad de certificación) debería cubrir cuestiones de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la prestación de servicios (véase 5.22).

Gestión de claves

La gestión adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Un sistema de gestión de claves debería basarse en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) emitir y obtener certificados de clave pública;

c) distribuir claves a las entidades previstas, incluido cómo activar las claves cuando se reciben;

d) almacenar claves, incluida la forma en que los usuarios autorizados obtienen acceso a las claves;

e) cambiar o actualizar las claves, incluidas las reglas sobre cuándo cambiar las claves y cómo se hará;

f) tratar con claves comprometidas;

g) revocación de claves, incluido cómo retirar o desactivar claves [p. cuando las claves se han visto comprometidas o cuando un usuario deja una organización (en cuyo caso las claves también deberían archivarse)];

h) recuperar claves perdidas o dañadas;

i) realizar copias de seguridad o archivar claves;

j) destrucción de llaves;

k) registro y auditoría de actividades clave relacionadas con la gestión;

l) establecer fechas de activación y desactivación de claves para que las claves solo se puedan usar durante el período de tiempo de acuerdo con las reglas de la organización sobre administración de claves;

m) gestionar solicitudes legales de acceso a claves criptográficas (por ejemplo, se puede exigir que la información cifrada esté disponible sin cifrar como prueba en un caso judicial).

Todas las claves criptográficas deberían protegerse contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado y la divulgación. El equipo utilizado para generar, almacenar y archivar claves debería protegerse físicamente.

Además de la integridad, para muchos casos de uso, también se debería considerar la autenticidad de las claves públicas.

Otra información

La autenticidad de las claves públicas generalmente se aborda mediante procesos de administración de claves públicas que utilizan autoridades de certificación y certificados de clave pública, pero también es posible abordarla mediante el uso de tecnologías como la aplicación de procesos manuales para claves de números pequeños.

La criptografía se puede utilizar para lograr diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad: uso de cifrado de información para proteger información sensible o crítica, ya sea almacenada o transmitida;

b) integridad o autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Usar algoritmos con el fin de verificar la integridad de los archivos;

c) no repudio: utilizar técnicas criptográficas para proporcionar evidencia de la ocurrencia o no ocurrencia de un evento o acción;

d) autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso o realizan transacciones con usuarios, entidades y recursos del sistema.

La serie ISO/IEC 11770 proporciona más información sobre la gestión de claves.

8.25 Ciclo de vida de desarrollo seguro

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Seguridad_en_sistemas_y_redes	#protección

Control

Deberían establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.

Propósito

Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.

Guía

El desarrollo seguro es un requisito para crear un servicio, una arquitectura, un software y un sistema seguros. Para lograrlo, se deberían considerar los siguientes aspectos:

a) separación de los entornos de desarrollo, prueba y producción (véase 8.31);

b) orientación sobre la seguridad en el ciclo de vida del desarrollo de software:

1) seguridad en la metodología de desarrollo de software (véase 8.28 y 8.27);

2) pautas de codificación segura para cada lenguaje de programación utilizado (véase 8.28);

c) requisitos de seguridad en la fase de especificación y diseño (véase 5.8);

d) puntos de control de seguridad en proyectos (véase 5.8);

e) pruebas de sistema y seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración (véase 8.29);

f) repositorios seguros para el código fuente y la configuración (véase 8.4 y 8.9);

g) seguridad en el control de versiones (véase 8.32);

h) conocimiento y capacitación en seguridad de la aplicación requeridos (véase 8.28);

i) la capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades (véase 8.28);

j) requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (véase 5.32).

Si se subcontrata el desarrollo, la organización debería asegurarse de que el proveedor cumpla con las reglas de la organización para el desarrollo seguro (véase 8.30).

Otra información

El desarrollo también puede tener lugar dentro de aplicaciones, como aplicaciones de oficina, secuencias de comandos, navegadores y bases de datos.

8.26 Requisitos de seguridad de la aplicación

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Seguridad_en_sistemas_y_redes	#Protección #Defensa

Control

Los requisitos de seguridad de la información deberían identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

Propósito

Para garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

Guía

Generalidades

Deberían identificarse y especificarse los requisitos de seguridad de las aplicaciones. Estos requisitos generalmente se determinan a través de una evaluación de riesgos. Los requisitos deberían desarrollarse con el apoyo de especialistas en seguridad de la información.

Los requisitos de seguridad de la aplicación pueden cubrir una amplia gama de temas, según el propósito de la aplicación.

Los requisitos de seguridad de la aplicación deberían incluir, según corresponda:

a) nivel de confianza en la identidad de las entidades [por ejemplo, mediante autenticación (véase 5.17, 8.2 y 8.5)];

b) identificar el tipo de información y el nivel de clasificación a ser procesado por la aplicación;

c) necesidad de segregación de acceso y nivel de acceso a datos y funciones en la aplicación;

d) resiliencia contra ataques maliciosos o interrupciones no intencionales [p. protección contra desbordamiento de búfer o inyecciones de lenguaje de consulta estructurado (SQL)];

e) requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción;

f) necesidad de privacidad asociada con todas las partes involucradas;

g) los requisitos de protección de cualquier información confidencial;

h) protección de datos en proceso, en tránsito y en reposo;

i) necesidad de cifrar de forma segura las comunicaciones entre todas las partes involucradas;

j) controles de entrada, incluidas verificaciones de integridad y validación de entrada;

k) controles automatizados (por ejemplo, límites de aprobación o aprobaciones dobles);

l) controles de salida, considerando también quién puede acceder a las salidas y su autorización;

m) restricciones en torno al contenido de los campos de "texto libre", ya que pueden conducir al almacenamiento no controlado de datos confidenciales (por ejemplo, datos personales);

n) requisitos derivados del proceso de negocio, tales como registro y seguimiento de transacciones, requisitos de no repudio;

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

p) manejo de mensajes de error.

Servicios transaccionales

Además, para las aplicaciones que ofrecen servicios transaccionales entre la organización y un socio, se debería considerar lo siguiente al identificar los requisitos de seguridad de la información:

a) el nivel de confianza que cada parte requiere en la identidad reclamada de cada uno;

b) el nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para la identificación de la falta de integridad (por ejemplo, verificación de redundancia cíclica, hashing, firmas digitales);

c) procesos de autorización asociados con quién puede aprobar contenidos, emitir o firmar documentos transaccionales clave;

d) confidencialidad, integridad, prueba de envío y recepción de documentos clave y no repudio (por ejemplo, contratos asociados a procesos de licitación y contratación);

e) la confidencialidad e integridad de cualquier transacción (por ejemplo, pedidos, detalles de la dirección de entrega y confirmación de recibos);

f) requisitos sobre cuánto tiempo mantener la confidencialidad de una transacción;

g) seguros y otros requisitos contractuales.

Aplicaciones de pago y pedidos electrónicos

Además, para aplicaciones que involucren pedidos y pagos electrónicos, se debería considerar lo siguiente:

a) requisitos para mantener la confidencialidad e integridad de la información de la orden;

b) el grado de verificación apropiado para verificar la información de pago proporcionada por un cliente;

c) evitar la pérdida o duplicación de información de transacciones;

d) almacenar los detalles de la transacción fuera de cualquier entorno de acceso público (por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización, y no retenida ni expuesta en medios de almacenamiento electrónico directamente accesibles desde Internet);

e) cuando se utiliza una autoridad de confianza (por ejemplo, con el fin de emitir y mantener firmas o certificados digitales), la seguridad se integra y se incorpora a lo largo de todo el proceso de gestión de firmas o certificados de extremo a extremo.

Varias de las consideraciones anteriores pueden abordarse mediante la aplicación de la criptografía (véase 8.24), teniendo en cuenta los requisitos legales (véase 5.31 a 5.36, especialmente véase 5.31 para la legislación criptográfica).

Otra información

Las aplicaciones accesibles a través de las redes están sujetas a una variedad de amenazas relacionadas con la red, como actividades fraudulentas, disputas de contratos o divulgación de información al público; transmisión incompleta, enrutamiento incorrecto, alteración, duplicación o reproducción de mensajes no autorizados. Por lo tanto, las evaluaciones de riesgo detalladas y la determinación cuidadosa de los controles son indispensables. Los controles requeridos a menudo incluyen métodos criptográficos para la autenticación y la seguridad de la transferencia de datos.

Puede encontrar más información sobre la seguridad de las aplicaciones en la serie ISO/IEC 27034.

8.27 Principios de ingeniería y arquitectura de sistemas seguros

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Seguridad_en_sistemas_y_redes	#Protección

Control

Los principios para diseñar sistemas seguros deberían establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.

Propósito

Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

Guía

Los principios de ingeniería de seguridad deberían establecerse, documentarse y aplicarse a las actividades de ingeniería de sistemas de información. La seguridad debería diseñarse en todas las capas de la arquitectura (negocios, datos, aplicaciones y tecnología). La nueva tecnología debería analizarse en busca de riesgos de seguridad y el diseño debería revisarse frente a patrones de ataque conocidos.

Los principios de ingeniería segura brindan orientación sobre las técnicas de autenticación de usuarios, el control seguro de sesiones y la validación y desinfección de datos.

Los principios de ingeniería de sistemas seguros deberían incluir el análisis de:

a) la gama completa de controles de seguridad necesarios para proteger la información y los sistemas contra las amenazas identificadas;

b) las capacidades de los controles de seguridad para prevenir, detectar o responder a eventos de seguridad;

c) controles de seguridad específicos requeridos por procesos comerciales particulares (por ejemplo, cifrado de información confidencial, verificación de integridad y firma digital de información);

d) dónde y cómo se aplicarán los controles de seguridad (por ejemplo, mediante la integración con una arquitectura de seguridad y la infraestructura técnica);

e) cómo los controles de seguridad individuales (manuales y automatizados) funcionan juntos para producir un conjunto integrado de controles.

Los principios de ingeniería de seguridad deberían tener en cuenta:

a) la necesidad de integrarse con una arquitectura de seguridad;

b) infraestructura de seguridad técnica [p. infraestructura de clave pública (PKI), gestión de identidad y acceso (GIA), prevención de fuga de datos y gestión de acceso dinámico];

c) capacidad de la organización para desarrollar y soportar la tecnología elegida;

d) costo, tiempo y complejidad de cumplir con los requisitos de seguridad;

e) buenas prácticas actuales.

La ingeniería de sistemas seguros debería implicar:

a) el uso de principios de arquitectura de seguridad, tales como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación predeterminada", "fallo seguro", "desconfiar de la entrada de aplicaciones externas", "seguridad en implementación", "asumir incumplimiento", "privilegio mínimo", "facilidad de uso y administración" y "funcionalidad mínima";

b) una revisión del diseño orientada a la seguridad para ayudar a identificar las vulnerabilidades de la seguridad de la información, asegurar que se especifiquen los controles de seguridad y cumplir con los requisitos de seguridad;

c) documentación y reconocimiento formal de los controles de seguridad que no cumplen plenamente los requisitos (por ejemplo, debido a requisitos de seguridad superiores);

d) endurecimiento de los sistemas.

La organización debería considerar principios de "confianza cero" tales como:

a) suponiendo que los sistemas de información de la organización ya han sido violados y, por lo tanto, no dependen solo de la seguridad del perímetro de la red;

b) emplear un enfoque de "nunca confiar y siempre verificar" para el acceso a los sistemas de información;

c) garantizar que las solicitudes a los sistemas de información estén encriptadas de extremo a extremo;

d) verificar cada solicitud a un sistema de información como si se originara en una red externa abierta, incluso si estas solicitudes se originaron internamente en la organización (es decir, no confiar automáticamente en nada dentro o fuera de sus perímetros);

e) utilizando técnicas de control de acceso dinámico y de "privilegio mínimo" (véase 5.15, 5.18 y 8.2). Esto incluye autenticar y autorizar solicitudes de información o a sistemas basados en información contextual como información de autenticación (véase 5.17), identidades de usuario (véase 5.16), datos sobre el dispositivo de punto final del usuario y clasificación de datos (véase 5.12);

f) siempre autenticar a los solicitantes y siempre validar las solicitudes de autorización a los sistemas de información en función de la información, incluida la información de autenticación (véase 5.17) y las identidades de los usuarios (5.16), los datos sobre el dispositivo de punto final del usuario y la clasificación de datos (véase 5.12), por ejemplo, hacer cumplir una autenticación fuerte (por ejemplo, multifactor, véase 8.5).

Los principios de ingeniería de seguridad establecidos deberían aplicarse, cuando corresponda, al desarrollo subcontratado de sistemas de información a través de contratos y otros acuerdos vinculantes entre la organización y el proveedor a quien la organización subcontrata. La organización debería asegurarse de que las prácticas de ingeniería de seguridad de los proveedores se alineen con las necesidades de la organización.

Los principios de ingeniería de seguridad y los procedimientos de ingeniería establecidos deberían revisarse periódicamente para garantizar que contribuyan efectivamente a mejorar los estándares de seguridad dentro del proceso de ingeniería. También deberían revisarse periódicamente para garantizar que permanezcan actualizados en términos de combatir cualquier nueva amenaza potencial y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Otra información

Los principios de ingeniería segura se pueden aplicar al diseño o configuración de una variedad de técnicas, como:

— tolerancia a fallas y otras técnicas de resiliencia;

— segregación (por ejemplo, mediante virtualización o contenedorización);

— resistencia a la manipulación.

Se pueden utilizar técnicas de virtualización seguras para evitar la interferencia entre aplicaciones que se ejecutan en el mismo dispositivo físico. Si un atacante pone en peligro una instancia virtual de una aplicación, solo esa instancia se ve afectada. El ataque no tiene efecto en ninguna otra aplicación o datos.

Las técnicas de resistencia a la manipulación pueden utilizarse para detectar la manipulación de contenedores de información, ya sea física (por ejemplo, una alarma antirrobo) o lógica (por ejemplo, un archivo de datos). Una característica de tales técnicas es que existe un registro del intento de manipulación del contenedor. Además, el control puede evitar la extracción exitosa de datos a través de su destrucción (por ejemplo, se puede eliminar la memoria del dispositivo).

8.28 Codificación segura

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Seguridad_en_sistemas_y_redes	#Protección

Control

Los principios de codificación segura deberían aplicarse al desarrollo de software.

Propósito

Garantizar que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información en el software.

Guía

Generalidades

La organización debería establecer procesos en toda la organización 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 deberían extenderse para cubrir los componentes de software de terceros y el software de código abierto.

La organización debería monitorear las amenazas del mundo real y actualizar el asesoramiento y la información sobre las vulnerabilidades del software para guiar los principios de codificación segura de la organización a través de la mejora y el aprendizaje continuos. Esto puede ayudar a garantizar que se implementen prácticas de codificación seguras y efectivas para combatir el panorama de amenazas que cambia rápidamente.

Planificación y antes de codificar

Los principios de codificación segura deberían usarse tanto para nuevos desarrollos como en escenarios de reutilización. Estos principios deberían aplicarse a las actividades de desarrollo tanto dentro de la organización como para los productos y servicios que la organización proporciona a otros. La planificación y los requisitos previos antes de la codificación deberían incluir:

a) expectativas específicas de la organización y principios aprobados para la codificación segura que se utilizará para desarrollos de código internos y externos;

b) prácticas y defectos de codificación comunes e históricos que conducen a vulnerabilidades de seguridad de la información;

c) configurar herramientas de desarrollo, como entornos de desarrollo integrados (IDE), para ayudar a hacer cumplir la creación de código seguro;

d) seguir la orientación emitida por los proveedores de herramientas de desarrollo y entornos de ejecución, según corresponda;

e) mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores);

f) calificación de los desarrolladores en la escritura de código seguro;

g) diseño y arquitectura seguros, incluido el modelado de amenazas;

h) normas de codificación seguras y, cuando corresponda, exigir su uso;

i) uso de ambientes controlados para el desarrollo.

Durante la codificación

Las consideraciones durante la codificación deberían incluir:

a) prácticas de codificación seguras específicas para los lenguajes y técnicas de programación que se utilizan;

b) utilizar técnicas de programación seguras, como programación en pares, refactorización, revisión por pares, iteraciones de seguridad y desarrollo basado en pruebas;

c) utilizando técnicas de programación estructurada;

d) documentar el código y eliminar los defectos de programación, lo que puede permitir que se exploten las vulnerabilidades de seguridad de la información;

e) prohibir el uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, ejemplos de código no aprobados y servicios web no autenticados).

Las pruebas deberían realizarse durante y después del desarrollo (véase 8.29). Los procesos de prueba de seguridad de aplicaciones estáticas (SAST) pueden identificar vulnerabilidades de seguridad en el software.

Antes de que el software entre en funcionamiento, se debería evaluar lo siguiente:

a) superficie de ataque y el principio de privilegio mínimo;

b) realizar un análisis de los errores de programación más comunes y documentar que estos han sido mitigados.

Revisión y mantenimiento

Después de que el código se haya hecho operativo:

a) las actualizaciones deberían empaquetarse e implementarse de forma segura;

b) se deberían manejar las vulnerabilidades de seguridad de la información informadas (véase 8.8);

c) los errores y los ataques sospechosos deberían registrarse y los registros deberían revisarse periódicamente para hacer los ajustes necesarios al código;

d) el código fuente debería protegerse contra el acceso no autorizado y la manipulación (por ejemplo, mediante el uso de herramientas de gestión de la configuración, que suelen proporcionar funciones como control de acceso y control de versiones).

Si utiliza herramientas y bibliotecas externas, la organización debería considerar:

a) garantizar que las bibliotecas externas se gestionen (por ejemplo, manteniendo un inventario de las bibliotecas utilizadas y sus versiones) y se actualicen regularmente con los ciclos de publicación;

b) selección, autorización y reutilización de componentes bien examinados, en particular componentes de autenticación y criptográficos;

c) la licencia, seguridad e historial de los componentes externos;

d) garantizar que el software se pueda mantener, rastrear y provenir de fuentes comprobadas y confiables;

e) disponibilidad a largo plazo de recursos y artefactos para el desarrollo.

Cuando sea necesario modificar un paquete de software, se deberían considerar los siguientes puntos:

a) el riesgo de que los controles incorporados y los procesos de integridad se vean comprometidos;

b) si se deberá obtener el consentimiento del vendedor;

c) la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones estándar del programa;

d) el impacto si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios;

e) compatibilidad con otro software en uso.

Otra información

Un principio rector es garantizar que el código relevante para la seguridad se invoque cuando sea necesario y sea resistente a la manipulación. Los programas instalados a partir de código binario compilado también tienen estas propiedades, pero solo para los datos contenidos en la aplicación. Para los lenguajes interpretados, el concepto solo funciona cuando el código se ejecuta en un servidor que de otro modo es inaccesible para los usuarios y los procesos que lo usan, y que sus datos se mantienen en una base de datos protegida de manera similar. Por ejemplo, el código interpretado se puede ejecutar en un servicio en la nube donde el acceso al código requiere privilegios de administrador. Dicho acceso de administrador debería estar protegido por mecanismos de seguridad, como los principios de administración justo a tiempo y la autenticación sólida. Si el propietario de la aplicación puede acceder a los scripts mediante acceso remoto directo al servidor, en principio también puede hacerlo un atacante. Los servidores web deberían configurarse para evitar la exploración de directorios en tales casos.

El código de la aplicación se diseña mejor asumiendo que siempre está sujeto a ataques, por error o acción maliciosa. Además, las aplicaciones críticas pueden diseñarse para ser tolerantes a fallas internas. Por ejemplo, la salida de un algoritmo complejo puede verificarse para asegurarse de que se encuentra dentro de límites seguros antes de que los datos se utilicen en una aplicación como una aplicación crítica financiera o de seguridad. El código que realiza las comprobaciones de límites es simple y, por lo tanto, mucho más fácil de probar que es correcto.

Algunas aplicaciones web son susceptibles a una variedad de vulnerabilidades que son introducidas por un diseño y una codificación deficientes, como la inyección de bases de datos y los ataques de secuencias de comandos entre sitios. En estos ataques, las solicitudes pueden manipularse para abusar de la funcionalidad del servidor web.

Puede encontrar más información sobre la evaluación de la seguridad de las TIC en la serie ISO/IEC 15408.

8.29 Pruebas de seguridad en desarrollo y aceptación.

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Aseguramiento_de_seguridad_de_la_información #Seguridad_en_sistemas_y_redes	#Protección

Control

Los procesos de prueba de seguridad deberían definirse e implementarse en el ciclo de vida del desarrollo.

Propósito

Para validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción.

Guía

Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deberían probarse y verificarse minuciosamente durante los procesos de desarrollo. Las pruebas de seguridad deberían ser una parte integral de las pruebas de sistemas o componentes.

Las pruebas de seguridad deberían realizarse frente a un conjunto de requisitos, que pueden expresarse como funcionales o no funcionales. Las pruebas de seguridad deberían incluir pruebas de:

a) funciones de seguridad [p. autenticación de usuarios (véase 8.5), restricción de acceso (véase 8.3) y uso de criptografía (véase 8.24)];

b) codificación segura (véase 8.28);

c) configuraciones seguras (véase 8.9, 8.20 y 8.22) incluyendo la de sistemas operativos, firewalls y otros componentes de seguridad.

Los planes de prueba deberían determinarse utilizando un conjunto de criterios. El alcance de las pruebas debería ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo. El plan de prueba debería incluir:

a) cronograma detallado de actividades y pruebas;

b) insumos y productos esperados bajo una variedad de condiciones;

c) criterios para evaluar los resultados;

d) decisión de acciones adicionales según sea necesario.

La organización puede aprovechar las herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidades, y debería verificar la corrección de los defectos relacionados con la seguridad.

Para los desarrollos internos, estas pruebas deberían ser realizadas inicialmente por el equipo de desarrollo. Luego se deberían realizar pruebas de aceptación independientes para garantizar que el sistema funcione como se espera y solo como se esperaba (véase 5.8). Se debería considerar lo siguiente:

a) realizar actividades de revisión de código como un elemento relevante para probar fallas de seguridad, incluidas entradas y condiciones no anticipadas;

b) realizar un escaneo de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema;

c) realizar pruebas de penetración para identificar código y diseño inseguros.

Para los componentes de compra y desarrollo subcontratados, se debería seguir un proceso de adquisición.

Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados (véase 5.20). Los productos y servicios deberían evaluarse según estos criterios antes de la adquisición.

Las pruebas deberían realizarse en un entorno de prueba que coincida lo más posible con el entorno de producción objetivo para garantizar que el sistema no introduzca vulnerabilidades en el entorno de la organización y que las pruebas sean confiables (véase 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 deberían considerar las pruebas y el monitoreo de los entornos de prueba, las herramientas y las tecnologías para garantizar la eficacia de las pruebas. Las mismas consideraciones se aplican al monitoreo de los sistemas de monitoreo implementados en entornos de desarrollo, prueba y producción. Se necesita juicio, guiado por la sensibilidad de los sistemas y los datos, para determinar cuántas capas de meta-test son útiles.

8.30 Desarrollo tercerizado

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Seguridad_en_sistemas_y_redes #Seguridad_en_las_aplicaciones #Seguridad_en_las_relaciones_con_proveedores	#Gobernanza_y_Ecosistema #Protección

Control

La organización debería dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

Propósito

Para garantizar que las medidas de seguridad de la información requeridas por la organización se implementen en el desarrollo de sistemas subcontratados.

Guía

Cuando se subcontrata el desarrollo del sistema, la organización debería comunicar y acordar los requisitos y expectativas, y monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con estas expectativas. Se deberían considerar los siguientes puntos en toda la cadena de suministro externa de la organización:

a) acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado (véase 5.32);

b) requisitos contractuales para prácticas seguras de diseño, codificación y pruebas (véanse 8.25 a 8.29);

c) provisión del modelo de amenaza a considerar por desarrolladores externos;

d) pruebas de aceptación para la calidad y exactitud de los entregables (véase 8.29);

e) provisión de evidencia de que se han establecido niveles mínimos aceptables de seguridad y capacidades de privacidad (por ejemplo, informes de aseguramiento);

f) provisión de evidencia de que se han aplicado suficientes pruebas para protegerse contra la presencia de contenido malicioso (tanto intencional como no intencional) en el momento de la entrega;

g) provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas;

h) acuerdos de depósito en garantía para el código fuente del software (por ejemplo, si el proveedor cierra);

i) derecho contractual a auditar procesos y controles de desarrollo;

j) requisitos de seguridad para el entorno de desarrollo (véase 8.31);

k) teniendo en cuenta la legislación aplicable (por ejemplo, sobre protección de datos personales).

Otra información

Se puede encontrar más información sobre las relaciones con los proveedores en la serie ISO/IEC 27036.

8.31 Separación de los entornos de desarrollo, prueba y producción

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Seguridad_en_sistemas_y_redes	#Protección

Control

Los entornos de desarrollo, prueba y producción deberían estar separados y protegidos.

Propósito

Para proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.

Guía

Debería identificarse e implementarse el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción.

Se deberían considerar los siguientes elementos:

a) separar adecuadamente los sistemas de desarrollo y producción y operarlos en diferentes dominios (por ejemplo, en entornos físicos o virtuales separados);

b) definir, documentar e implementar reglas y autorizaciones para el despliegue de software desde el estado de desarrollo hasta el de producción;

c) probar los cambios en los sistemas de producción y las aplicaciones en un entorno de pruebas o etapas antes de aplicarlos a los sistemas de producción (véase 8.29);

d) no realizar pruebas en entornos de producción excepto en circunstancias que hayan sido definidas y aprobadas;

e) compiladores, editores y otras herramientas de desarrollo o programas de utilidad que no sean accesibles desde los sistemas de producción cuando no se requieran;

f) mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error;

g) no copiar información confidencial en los entornos del sistema de desarrollo y prueba a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y prueba.

En todos los casos, los entornos de desarrollo y pruebas deberían protegerse teniendo en cuenta:

a) aplicación de parches y actualización de todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y bibliotecas);

b) configuración segura de sistemas y software;

c) control de acceso a los ambientes;

d) seguimiento de cambios en el entorno y código almacenado en el mismo;

e) monitoreo seguro de los ambientes;

f) realizar copias de seguridad de los entornos.

Una sola persona no debería tener la capacidad de realizar cambios tanto en el desarrollo como en la producción sin una revisión y aprobación previas. Esto se puede lograr, por ejemplo, mediante la segregación de los derechos de acceso o mediante reglas supervisadas. En situaciones excepcionales, se deberían implementar medidas adicionales como registro detallado y monitoreo en tiempo real para detectar y actuar sobre cambios no autorizados.

Otra información

Sin medidas y procedimientos adecuados, los desarrolladores y probadores que tienen acceso a los sistemas de producción pueden presentar riesgos significativos (por ejemplo, modificación no deseada de archivos o del entorno del sistema, falla del sistema, ejecución de código no autorizado y no probado en sistemas de producción, divulgación de datos confidenciales, integridad de datos y problemas de disponibilidad). Es necesario mantener un entorno conocido y estable en el que realizar pruebas significativas y evitar el acceso inapropiado del desarrollador al entorno de producción.

Las medidas y los procedimientos incluyen roles cuidadosamente diseñados junto con la implementación de requisitos de segregación de tareas y la implementación de procesos de monitoreo adecuados.

El personal de desarrollo y pruebas también representa una amenaza para la confidencialidad de la información de producción.

Las actividades de desarrollo y prueba pueden provocar cambios no deseados en el software o la información si comparten el mismo entorno informático. Por lo tanto, es deseable separar los entornos de desarrollo, prueba y producción para reducir el riesgo de cambio accidental o acceso no autorizado al software de producción y los datos comerciales (consulte 8.33 para la protección de la información de prueba).

En algunos casos, la distinción entre entornos de desarrollo, prueba y producción puede desdibujarse deliberadamente y las pruebas pueden llevarse a cabo en un entorno de desarrollo o a través de implementaciones controladas para usuarios o servidores reales (por ejemplo, una pequeña población de usuarios piloto). En algunos casos, la prueba del producto puede ocurrir mediante el uso en vivo del producto dentro de la organización. Además, para reducir el tiempo de inactividad de las implementaciones en vivo, se pueden admitir dos entornos de producción idénticos donde solo uno está en vivo en cualquier momento.

Son necesarios procesos de apoyo para el uso de datos de producción en entornos de desarrollo y prueba (8.33).

Las organizaciones también pueden considerar la orientación proporcionada en esta sección para los entornos de capacitación al realizar la capacitación del usuario final.

8.32 Gestión de cambios

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_las_aplicaciones #Seguridad_en_sistemas_y_redes	#Protección

Control

Los cambios en las instalaciones de procesamiento de información y los sistemas de información deberían estar sujetos a procedimientos de gestión de cambios.

Propósito

Preservar la seguridad de la información al ejecutar cambios.

Guía

La introducción de nuevos sistemas y cambios importantes en los sistemas existentes debería seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación administrada.

Deberían existir responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios deberían documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de procesamiento de información y los sistemas de información, durante todo el ciclo de vida del desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores.

Siempre que sea factible, deberían integrarse los procedimientos de control de cambios para la infraestructura y el software de las TIC.

Los procedimientos de control de cambios deberían incluir:

a) planificar y evaluar el impacto potencial de los cambios considerando todas las dependencias;

b) autorización de cambios;

c) comunicar los cambios a las partes interesadas pertinentes;

d) pruebas y aceptación de pruebas para los cambios (véase 8.29);

e) implementación de cambios, incluidos los planes de implementación;

f) consideraciones de emergencia y contingencia, incluidos los procedimientos de respaldo;

g) mantener registros de cambios que incluyan todo lo anterior;

h) asegurar que la documentación operativa (véase 5.37) y los procedimientos del usuario se cambien según sea necesario para seguir siendo apropiados;

i) garantizar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación (véase 5.30) se cambien según sea necesario para seguir siendo apropiados.

Otra información

El control inadecuado de los cambios en las instalaciones de procesamiento de información y los sistemas de información es una causa común de fallas en el sistema o la seguridad. Los cambios en el entorno de producción, especialmente cuando se transfiere software del entorno de desarrollo al operativo, pueden afectar la integridad y disponibilidad de las aplicaciones.

Cambiar el software puede afectar el entorno de producción y viceversa.

Las buenas prácticas incluyen la prueba de los componentes de las TIC en un entorno separado de los entornos de producción y desarrollo (véase 8.31). Esto proporciona un medio para tener control sobre el nuevo software y permitir una protección adicional de la información operativa que se utiliza con fines de prueba. Esto debería incluir parches, paquetes de servicio y otras actualizaciones.

El entorno de producción incluye sistemas operativos, bases de datos y plataformas de middleware. El control debería aplicarse para cambios de aplicaciones e infraestructuras.

8.33 Información para pruebas

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad	#Proteger	#Protección_de_la_información	#Protección

Control

La información de las pruebas debería seleccionarse, protegerse y gestionarse adecuadamente.
Propósito

Para garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas.

Guía

La información de prueba debería seleccionarse para garantizar la confiabilidad de los resultados de las pruebas y la confidencialidad de la información operativa relevante. La información confidencial (incluida la información de identificación personal) no debería copiarse en los entornos de desarrollo y prueba (consulte 8.31).

Se deberían aplicar las siguientes pautas para proteger las copias de la información operativa, cuando se utilizan con fines de prueba, ya sea que el entorno de prueba se construya internamente o en un servicio en la nube:

a) aplicar los mismos procedimientos de control de acceso a los entornos de prueba que los que se aplican a los entornos operativos;

b) tener una autorización separada cada vez que se copia información operativa a un entorno de prueba;

c) registrar la copia y el uso de información operativa para proporcionar una pista de auditoría;

d) proteger la información confidencial mediante eliminación o enmascaramiento (véase 8.11) si se usa para pruebas;

e) eliminar correctamente (véase 8.10) la información operativa de un entorno de prueba inmediatamente después de que se complete la prueba para evitar el uso no autorizado de la información de la prueba.

La información de la prueba debería almacenarse de forma segura (para evitar la manipulación, que de lo contrario puede generar resultados no válidos) y solo debería usarse para fines de prueba.

Otra información

Las pruebas del sistema y de aceptación pueden requerir volúmenes sustanciales de información de prueba que estén lo más cerca posible de la información operativa.

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_sistemas_y_redes #Protección_de_la_información	#Gobernanza_y_Ecosistema #Protección

Control

Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deberían planificarse y acordarse entre el evaluador y la gerencia correspondiente.

Propósito

Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y procesos comerciales.

Guía

Se deberían observar las siguientes pautas:

a) acordar solicitudes de auditoría para el acceso a sistemas y datos con la gestión adecuada;

b) acordar y controlar el alcance de las pruebas de auditoría técnica;

c) limitar las pruebas de auditoría al acceso de solo lectura al software y los datos. Si el acceso de solo lectura no está disponible para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor;

d) si se otorga el acceso, establecer y verificar los requisitos de seguridad (por ejemplo, antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (por ejemplo, computadoras portátiles o tabletas) antes de permitir el acceso;

e) solo permitir el acceso que no sea de solo lectura para copias aisladas de archivos del sistema, eliminándolos cuando se complete la auditoría, o brindándoles la protección adecuada si existe la obligación de mantener dichos archivos bajo los requisitos de documentación de auditoría;

f) identificar y acordar solicitudes de procesamiento especial o adicional, como ejecutar herramientas de auditoría;

g) ejecutar pruebas de auditoría que puedan afectar la disponibilidad del sistema fuera del horario comercial;

h) supervisar y registrar todos los accesos con fines de auditoría y prueba.

Otra información

Las pruebas de auditoría y otras actividades de aseguramiento también pueden ocurrir en los sistemas de prueba y desarrollo, donde dichas pruebas pueden afectar, por ejemplo, la integridad del código o conducir a la divulgación de cualquier información confidencial que se encuentre en dichos entornos.

ANEXO A
(INFORMATIVO)

Uso de atributos

A.1 General

Este anexo proporciona una tabla para demostrar el uso de atributos como una forma de crear diferentes vistas de los controles. Los ejemplos del uso de estos atributos son los siguientes:

a) Tipos de control (#Preventivo, #Detectivo, #Correctivo)

b) Propiedades de seguridad de la información (#Confidencialidad, #Integridad, #Disponibilidad)

c) Conceptos de ciberseguridad (#Identificar, #Proteger, #Detectar, #Responder, #Recuperar)

d) Capacidades Operativas (#Gobernanza, #Gestión_de_activos, #Protección_de_la_Información, #Seguridad_de_recursos_humanos, #Seguridad_física, #Seguridad_de_sistemas_y_redes, #Seguridad_de_aplicaciones, #Configuraciones_seguras, #Gestión_de_identidades_y_accesos, #Gestión_de_amenazas_y_vulnerabilidades, #Continuidad, #Seguridad_de_las_relaciones_con_los_proveedores, #Legal_y_cumplimiento, #Gestión_de_eventos_de_seguridad_de_la_información, #Aseguramiento_de_seguridad_de_la_información).

e) Dominios de seguridad (#Gobernanza_y_ecosistema, #Protección, #Defensa, #Resiliencia)

La Tabla A.1 contiene una matriz de todos los controles en este documento con sus valores de atributos datos.

El filtrado o clasificación de la matriz se puede lograr mediante el uso de una herramienta, como una hoja de cálculo simple o una base de datos, que puede incluir más información como texto del control, guía, orientación o atributos específicos de la organización (véase A.2).

Tabla A.1 - Matriz de controles y valores de atributo

ISO/IEC 27002 Identificador de control	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	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y ecosistema # Resiliencia
5.2	Roles y responsabilidades de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y ecosistema #Protección #Resiliencia
5.3	Segregación de funciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernanza #Gestión de identidad y acceso	#Gobernanza y ecosistema
5.4	Responsabilidades de gestión	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y ecosistema

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.5	Contacto con autoridades	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resiliencia
5.6	Contacto con grupos de intereses especiales	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Gestión de Amenazas y vulnerabilidades	#Defensa #Resiliencia
5.8	Seguridad de la información en la gestión de proyectos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gobernanza	#Gobernanza y ecosistema #Protección
5.9	Inventario de información y otros activos asociados	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión de activos	#Gobernanza y ecosistema #Protección
5.10	Uso aceptable de información y otros activos asociados.	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información	#Gobernanza y ecosistema #Protección
5.11	Devolución de activos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos	#Proteccion

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.12	Clasificación de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Protección de la información	#Proteccion #Defensa
5.13	Etiquetado de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Protección de la información	#Defensa #Protección
5.14	Transferencia de información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información	#Proteccion
5.15	Control de acceso	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidades y accesos	#Proteccion
5.16	Gestión de identidad	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidades y accesos	#Proteccion
5.17	Información de autenticación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidades y accesos	#Proteccion
5.18	Derechos de acceso	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidades y accesos	#Proteccion
5.19	Seguridad de la información en las relaciones con proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con los proveedores	#Gobernanza y ecosistema #Protección

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con los proveedores	#Gobernanza y ecosistema #Protección
5.21	Gerente seguridad de la información en la cadena de suministro de las TIC	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con los proveedores	#Gobernanza y ecosistema #Protección
5.22	Seguimiento, revisión y gestión de cambios de los servicios de los proveedores.	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con los proveedores	#Gobernanza y ecosistema #Protección #Defensa #Aseguramiento de seguridad de la información
5.23	Seguridad de la información para el uso de servicios en la nube	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de las relaciones con los proveedores	#Gobernanza y ecosistema #Protección
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gobernanza #Gestión de eventos de seguridad de la información	#Defensa
5.25	Evaluación y decisión sobre eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar # Responder	#Gestión de eventos de seguridad de información	#Defensa

ISO/IEC 27002 Identificador de control	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	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gestión de eventos de seguridad de información	#Defensa
5.27	Aprender de los incidentes de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión de eventos de seguridad de información	#Defensa
5.28	Recolección de evidencia	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión de eventos de seguridad de información	#Defensa
5.29	Seguridad de la información durante la interrupción	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Continuidad	#Protección #Resiliencia
5.30	Preparación de las TIC para la continuidad del negocio	#Correctivo	#Disponibilidad	#Responder	#Continuidad	#Resiliencia
5.31	Recolección de evidencia	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Legal y cumplimiento	#Gobernanza y ecosistema # Protección
5.32	Seguridad de la información durante la interrupción	# Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Legal y cumplimiento	#Gobernanza y ecosistema
5.33	Preparación de las TIC para la continuidad empresarial	# Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Legal y cumplimiento #Gestión de activos #Protección de la información	#Defensa

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.34	Requisitos legales, estatutarios, reglamentarios y contractuales	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Protección de la información #Legal y cumplimiento	#Protección
5.35	Derechos de propiedad intelectual	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Aseguramiento de la seguridad de la información	#Gobernanza y ecosistema
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información.	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Legal y cumplimiento #Aseguramiento de la seguridad de la información	#Gobernanza y ecosistema
5.37	Procedimientos operativos documentados	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión de activos #Seguridad física #Seguridad de sistemas y redes #Seguridad de aplicaciones #Configuración segura #Gestión de identidad y acceso #Gestión de amenazas y vulnerabilidades #Continuidad #Gestión de eventos de seguridad de la información	#Gobernanza y ecosistema #Protección #Defensa
6.1	Selección	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos	#Gobernanza y ecosistema

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
6.2	Términos y condiciones de empleo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos	#Gobernanza y ecosistema
6.3	Concientización, educación y capacitación en seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos	#Gobernanza y ecosistema
6.4	Proceso disciplinario	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad de los recursos humanos	#Gobernanza y ecosistema
6.5	Responsabilidades después de la terminación o cambio de empleo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos #Gestión de activos	#Gobernanza y ecosistema
6.6	Acuerdos de confidencialidad o no divulgación	#Preventivo	#Confidencialidad	#Proteger	#Seguridad de los recursos humanos #Protección de la información #Relaciones con proveedores	#Gobernanza y ecosistema
6.7	Trabajo remoto	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información #Seguridad física #Seguridad de sistemas y redes	#Protección
6.8	Informes de eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión de eventos de seguridad de información	#Defensa

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
7.1	Perímetros de seguridad física	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.2	Entrada física	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de Identidad y Acceso	#Protección
7.3	Asegurar oficinas, salas e instalaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de activos	#Protección
7.4	Monitoreo de seguridad física	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad física	#Protección #Defensa
7.5	Protección contra amenazas físicas y ambientales	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.6	Trabajar en áreas seguras	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.7	Escritorio y pantalla limpios	#Preventivo	#Confidencialidad	#Proteger	#Seguridad física	#Protección
7.8	Emplazamiento y protección de equipos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de activos	#Protección

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
7.9	Seguridad de los activos fuera de las instalaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de activos	#Protección
7.10	Medios de almacenamiento	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de activos	#Protección
7.11	Servicios de suministro	#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad física	#Protección
7.12	Seguridad del cableado	#Preventivo	#Confidencialidad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.13	Mantenimiento de equipo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de activos	#Protección #Resiliencia
7.14	Eliminación segura o reutilización de equipos	#Preventivo	#Confidencialidad	#Proteger	#Seguridad física #Gestión de activos	#Protección
8.1	Dispositivos de punto final de usuario	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información	#Protección
8.2	Derechos de acceso privilegiado	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidad y acceso	#Protección
8.3	Restricción de acceso a la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidad y acceso	#Protección

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.4	Acceso al código fuente	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidad y acceso #Seguridad de aplicaciones #Configuración segura	#Protección
8.5	Autenticación segura	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de identidad y acceso	#Protección
8.6	Gestión de la capacidad	#Preventivo #Detectivo	#Integridad #Disponibilidad	#Identifcar #Proteger #Detectar	#Continuidad	#Gobernanza y ecosistema #Protección
8.7	Protección contra software malicioso	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad de sistemas y redes #Protección de la información	#Protección #Defensa
8.8	Gestión de vulnerabilidades técnicas	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión de amenazas y vulnerabilidades	#Gobernanza y ecosistema #Protección #Defensa
8.9	Gestión de la configuración	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	Configuración segura	#Protección
8.10	Eliminación de información	#Preventivo	#Confidencialidad	#Proteger	#Protección de la información #Legal y cumplimiento	#Protección
8.11	Enmascaramiento de datos	#Preventivo	#Confidencialidad	#Proteger	#Protección de la información	#Protección
8.12	Prevención de fuga de datos	#Preventivo #Detectivo	#Confidencialidad	#Proteger #Detectar	#Protección de la información	#Protección #Defensa

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.13	Respaldo de la información	#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Protección
8.14	Redundancia de las instalaciones de procesamiento de información	#Preventivo	#Disponibilidad	#Proteger	#Continuidad #Gestión de activos	#Protección Resiliencia
8.15	Inicio de sesión	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión de eventos de seguridad de la información.	#Protección #Defensa
8.16	Actividades de monitoreo	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión de eventos de seguridad de la información.	#Defensa
8.17	Sincronización de reloj	#Detectivo	#Integridad	#Proteger #Detectar	#Gestión de eventos de seguridad de la información.	#Protección #Defensa
8.18	Uso de programas de utilidad privilegiados	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de sistemas y redes #Configuración segura #Seguridad de aplicaciones	#Protección
8.19	Instalación de software en sistemas operativos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración segura #Seguridad de aplicaciones	#Protección
8.20	Seguridad en redes	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad de sistemas y redes	#Protección
8.21	Seguridad de los servicios de red	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de sistemas y redes	#Protección

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.22	Segregación de redes	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de sistemas y redes	#Protección
8.23	Filtrado web	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de sistemas y redes	#Protección
8.24	Uso de la criptografía	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración segura	#Protección
8.25	Ciclo de vida de desarrollo seguro	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de aplicaciones #Seguridad de sistemas y redes	#Protección
8.26	Requisitos de seguridad de la aplicación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de aplicaciones #Seguridad de sistemas y redes	#Protección #Defensa
8.27	Principios de arquitectura e ingeniería de sistemas seguros	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de aplicaciones #Seguridad de sistemas y redes	#Protección
8.28	Codificación segura	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de aplicaciones #Seguridad de sistemas y redes	#Protección

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.29	Pruebas de seguridad en desarrollo y aceptación.	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de aplicaciones #Aseguramiento de la seguridad de la información #Seguridad de sistemas y redes	#Protección
8.30	Desarrollo subcontratado	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Seguridad de sistemas y redes #Seguridad de aplicaciones #Seguridad en las relaciones con proveedores	#Gobernanza y ecosistema #Proteción
8.31	Separación de los entornos de desarrollo, prueba y producción	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de aplicaciones #Seguridad de sistemas y redes	#Protección
8.32	Gestión del cambio	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de aplicaciones #Seguridad de sistemas y redes	#Protección
8.33	Información de prueba	#Preventivo	#Confidencialidad #Integridad	#Proteger	#Protección de la información	#Protección
8.34	Protección de los sistemas de información durante las pruebas de auditoría	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de sistemas y redes #Protección de la información	#Gobernanza y ecosistema #Protección

La Tabla A.2 muestra un ejemplo de cómo crear una vista filtrando por un valor de atributo particular, en este caso #Correctivo.

Tabla A.2 — Vista de #Controles Correctivos

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de Control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.5	Contacto con autoridades	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identicar #Proteger #Responder #Recuperar	#Governanza	#Defensa #Resiliencia
5.6	Contacto con grupos de interés especial	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Governanza	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Gestión de amenazas y vulnerabilidades	#Defensa #Resiliencia
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Governanza #Gestión de eventos de seguridad de la información	#Defensa
5.26	Respuesta a incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gestión de eventos de seguridad de la información	#Defensa
5.28	Recolección de evidencia	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión de eventos de seguridad de la información	#Defensa

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de Control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.29	Seguridad de la información durante la interrupción	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Ressponder	#Continuidad	#Protección #Resiliencia
5.30	Preparación de las TIC para la continuidad del negocio	#Correctivo	#Disponibilidad	#Responder	#Continuidad	#Resiliencia
5.35	Revisión independiente de la seguridad de la información.	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Aseguramiento de la seguridad de la información	#Gobernanza y ecosistema
5.37	Procedimientos operativos documentados	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión de activos #Seguridad física #Seguridad de sistemas y redes #Seguridad de aplicaciones #Configuración segura #Gestión de identidad y acceso #Gestión de amenazas y vulnerabilidades #Continuidad #Gestión de eventos de seguridad de la información	#Gobernanza y ecosistema #Protección #Defensa
6.4	Proceso Disciplinario	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad de los recursos humanos	#Gobernanza y ecosistema

ISO/IEC 27002 Identificador de control	Nombre del control	Tipo de Control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.7	Protección contra software malicioso	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad de sistemas y redes #Protección de la información	#Protección #Defensa
8.13	Respaldo de la Información	#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Protección
8.16	Actividades de monitoreo	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión de eventos de seguridad de la información	#Defensa

A.2 Vistas organizacionales

Dado que los atributos se utilizan para crear diferentes vistas de los controles, las organizaciones pueden descartar los ejemplos de atributos propuestos en este documento y crear sus propios atributos con diferentes valores para abordar las necesidades específicas de la organización. Además, los valores asignados a cada atributo pueden diferir entre organizaciones, ya que las organizaciones pueden tener diferentes puntos de vista sobre el uso o la aplicabilidad del control o de los valores asociados al atributo (cuando los valores son específicos del contexto de la organización). El primer paso es comprender por qué es deseable un atributo específico de la organización. Por ejemplo, si una organización ha construido sus planes de tratamiento de riesgos [consulte ISO/IEC 27001:2013, 6.1.3 e)] en función de los eventos, puede desear asociar un atributo de escenario de riesgo a cada control en este documento.

El beneficio de tal atributo es acelerar el proceso de cumplimiento del requisito ISO/IEC 27001 relacionado con el tratamiento de riesgos, que consiste en comparar los controles determinados a través del proceso de tratamiento de riesgos (denominados controles "necesarios"), con aquellos en ISO/IEC 27001:2013, Anexo A (que se emiten en este documento) para garantizar que no se ha pasado por alto ningún control necesario.

Una vez que se conocen el propósito y los beneficios, el siguiente paso es determinar los valores de los atributos. Por ejemplo, la organización podría identificar 9 eventos:

1) pérdida o robo del dispositivo móvil;

2) pérdida o robo de las instalaciones de la organización;

3) fuerza mayor, vandalismo y terrorismo.

4) falla de software, hardware, energía, internet y comunicaciones;

5) fraude;

6) hacking;

7) divulgación;

8) incumplimiento de la ley;

9) ingeniería social.

El segundo paso se puede lograr asignando identificadores a cada evento (por ejemplo, E1, E2, ..., E9).

El tercer paso es copiar los identificadores de control y los nombres de control de este documento en una hoja de cálculo o base de datos y asociar los valores de atributo con cada control, recordando que cada control puede tener más de un valor de atributo.

El paso final es ordenar la hoja de cálculo o consultar la base de datos para extraer la información requerida.

Otros ejemplos de atributos organizacionales (y valores posibles) incluyen:

a) madurez (valores de la serie ISO/IEC 33000 u otros modelos de madurez);

b) estado de implementación (pendiente, en proceso, parcialmente implementado, completamente implementado);

c) prioridad (1, 2, 3, entre otros);

d) áreas organizacionales involucradas (seguridad, TIC, recursos humanos, alta dirección, entre otros);

e) eventos;

f) bienes involucrados;

g) construir y ejecutar, para diferenciar los controles utilizados en los diferentes pasos del ciclo de vida del servicio;

h) otros marcos con los que trabaja la organización o desde los que puede estar en transición.

ANEXO B
(INFORMATIVO)

Correspondencia con ISO/IEC 27002:2013

El propósito de este anexo es proporcionar compatibilidad con versiones anteriores de ISO/IEC 27002:2013 para las organizaciones que actualmente usan ese estándar y ahora desean hacer la transición a esta edición.

La Tabla B.1 proporciona la correspondencia de los controles especificados en los capítulos 5 a 8 con los de la norma ISO/IEC 27002:2013.

Tabla B.1 - Correspondencia entre los controles en este documento y los controles en ISO/IEC 27002:2013

Identificador de control ISO/IEC 27002	Identificador de control ISO/IEC 27002:2013	Nombre de control
5.1	05.1.1, 05.1.2	Políticas de seguridad de la información
5.2	06.1.1	Roles y responsabilidades de seguridad de la información
5.3	06.1.2	Segregación de funciones
5.4	07.2.1	Responsabilidades de gestión
5.5	06.1.3	Contacto con autoridades
5.6	06.1.4	Contacto con grupos de interés especial
5.7	Nuevo	Inteligencia de amenazas
5.8	06.1.5, 14.1.1	Seguridad de la información en la gestión de proyectos.
5.9	08.1.1, 08.1.2	Inventario de información y otros activos asociados
5.10	08.1.3, 08.2.3	Uso aceptable de la información y otros activos asociados
5.11	08.1.4	Devolución de activos
5.12	08.2.1	Clasificación de la información
5.13	08.2.2	Etiquetado de información
5.14	13.2.1, 13.2.2, 13.2.3	Transferencia de información
5.15	09.1.1, 09.1.2	Control de acceso
5.16	09.2.1	Gestión de identidad
5.17	09.2.4, 09.3.1, 09.4.3	Información de autenticación
5.18	09.2.2, 09.2.5, 09.2.6	Derechos de acceso
5.19	15.1.1	Seguridad de la información en las relaciones con los proveedores

Identificador de control ISO/IEC 27002	Identificador de control ISO/IEC 27002:2013	Nombre de control
5.20	15.1.2	Abordar la seguridad de la información en los acuerdos con los proveedores
5.21	15.1.3	Gestión de la seguridad de la información en la cadena de suministro de las TIC
5.22	15.2.1, 15.2.2	Seguimiento, revisión y gestión de cambios de servicios de proveedores
5.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
5.24	16.1.1	Planificación y preparación de la gestión de incidentes de seguridad de la información
5.25	16.1.4	Evaluación y decisión sobre eventos de seguridad de la información
5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprender de los incidentes de seguridad de la información
5.28	16.1.7	Recolección de evidencia
5.29	17.1.1, 17.1.2, 17.1.3	Seguridad de la información durante la interrupción
5.30	Nuevo	Preparación de las TIC para la continuidad del negocio
5.31	18.1.1, 18.1.5	Requisitos legales, estatutarios, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual
5.33	18.1.3	Protección de registros
5.34	18.1.4	Privacidad y protección de IIP
5.35	18.2.1	Revisión independiente de la seguridad de la información.
5.36	18.2.2, 18.2.3	Cumplimiento de políticas, normas y estándares de seguridad de la información
5.37	12.1.1	Procedimientos operativos documentados
6.1	07.1.1	Selección
6.2	07.1.2	Términos y condiciones de empleo
6.3	07.2.2	Concientización, educación y capacitación en seguridad de la información
6.4	07.2.3	Proceso Disciplinario
6.5	07.3.1	Responsabilidades después de la terminación o cambio de empleo
6.6	13.2.4	Acuerdos de confidencialidad o no divulgación
6.7	06.2.2	Trabajo remoto
6.8	16.1.2, 16.1.3	Informes de eventos de seguridad de la información
7.1	11.1.1	Perímetros físicos de seguridad
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Asegurar oficinas, salas e instalaciones
7.4	Nuevo	Monitoreo de seguridad física
7.5	11.1.4	Protección contra amenazas físicas y ambientales.

Identificador de control ISO/IEC 27002	Identificador de control ISO/IEC 27002:2013	Nombre de control
7.6	11.1.5	Trabajar en áreas seguras
7.7	11.2.9	Escritorio y pantalla limpios
7.8	11.2.1	Emplazamiento y protección de equipos
7.9	11.2.6	Seguridad de los activos fuera de las instalaciones
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Medios de almacenamiento
7.11	11.2.2	Servicios de suministro
7.12	11.2.3	Seguridad del cableado
7.13	11.2.4	Mantenimiento de equipo
7.14	11.2.7	Eliminación segura o reutilización de equipos
8.1	06.2.1, 11.2.8	Dispositivos de punto final de usuario
8.2	09.2.3	Derechos de acceso privilegiado
8.3	09.4.1	Restricción de acceso a la información
8.4	09.4.5	Acceso al código fuente
8.5	09.4.2	Autenticación segura
8.6	12.1.3	Gestión de capacidad
8.7	12.2.1	Protección contra software malicioso
8.8	12.6.1, 18.2.3	Gestión de vulnerabilidades técnicas
8.9	Nuevo	Gestión de la configuración
8.10	Nuevo	Eliminación de información
8.11	Nuevo	Enmascaramiento de datos
8.12	Nuevo	Prevención de fuga de datos
8.13	12.3.1	Respaldo de la información
8.14	17.2.1	Redundancia de las instalaciones de procesamiento de información
8.15	12.4.1, 12.4.2, 12.4.3	Inicio sesión
8.16	Nuevo	Actividades de seguimiento
8.17	12.4.4	Sincronización de reloj
8.18	09.4.4	Uso de programas de utilidad privilegiados
8.19	12.5.1, 12.6.2	Instalación de software en sistemas operativos
8.20	13.1.1	Seguridad en redes
8.21	13.1.2	Seguridad de los servicios de red.
8.22	13.1.3	Segregación de redes
8.23	Nuevo	Filtrado web
8.24	10.1.1, 10.1.2	Uso de criptografía
8.25	14.2.1	Ciclo de vida de desarrollo seguro
8.26	14.1.2, 14.1.3	Requisitos de seguridad de la aplicación
8.27	14.2.5	Principios de arquitectura e ingeniería de sistemas seguros
8.28	Nuevo	Codificación segura
8.29	14.2.8, 14.2.9	Pruebas de seguridad en desarrollo y aceptación.
8.30	14.2.7	Desarrollo subcontratado

Identificador de control ISO/IEC 27002	Identificador de control ISO/IEC 27002:2013	Nombre de control
8.31	12.1.4, 14.2.6	Separación de los entornos de desarrollo, prueba y producción
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestión del cambio
8.33	14.3.1	Información de prueba
8.34	12.7.1	Protección de los sistemas de información durante las pruebas de auditoría

La Tabla B.2 proporciona la correspondencia de los controles especificados en ISO/IEC 27002:2013 con los de este documento.

Tabla B.2 - Correspondencia entre los controles en ISO/IEC 27002:2013 y los controles en este documento

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002	Nombre de control según ISO/IEC 27002:2013
5		Políticas de seguridad de la información
5.1		Dirección de gestión para la seguridad de la información.
5.1.1	5.1	Políticas de seguridad de la información
5.1.2	5.1	Revisión de las políticas de seguridad de la información
6		Organización de la seguridad de la información.
6.1		Organización interna
6.1.1	5.2	Roles y responsabilidades 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 especial
6.1.5	5.8	Seguridad de la información en la gestión de proyectos.
6.2		Dispositivos móviles y teletrabajo
6.2.1	8.1	Política de dispositivos móviles
6.2.2	6.7	Teletrabajo
7		Seguridad de los recursos humanos
7.1		Antes del empleo
7.1.1	6.1	Selección
7.1.2	6.2	Términos y condiciones de empleo
7.2		Durante el empleo
7.2.1	5.4	responsabilidades de gestión

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002	Nombre de control según ISO/IEC 27002:2013
7.2.2	6.3	Concientización, educación y capacitación en seguridad de la información
7.2.3	6.4	Proceso Disciplinario
7.3		Terminación y cambio de empleo
7.3.1	6.5	Terminación o cambio de responsabilidades laborales
8		Gestión de activos
8.1		Responsabilidad por los activos
8.1.1	5.9	Inventario de activos
8.1.2	5.9	Propiedad de los activos
8.1.3	5.10	Uso aceptable de los activos
8.1.4	5.11	Devolución de activos
8.2		Clasificación de la información
8.2.1	5.12	Clasificación de la información
8.2.2	5.13	Etiquetado de información
8.2.3	5.10	manejo de activos
8.3		manejo de medios
8.3.1	7.10	Gestión de medios extraíbles
8.3.2	7.10	Eliminación de medios
8.3.3	7.10	Transferencia de medios físicos
9		Control de acceso
9.1		requisitos del negocio de control de acceso
9.1.1	5.15	Política de control de acceso
9.1.2	5.15	Acceso a redes y servicios de red
9.2		Gestión de acceso de usuarios
9.2.1	5.16	Alta y baja de usuario
9.2.2	5.18	Aprovisionamiento de acceso de usuarios
9.2.3	8.2	Gestión de derechos de acceso privilegiado
9.2.4	5.17	Gestión de la información secreta de autenticación de los usuarios
9.2.5	5.18	Revisión de los derechos de acceso de los usuarios
9.2.6	5.18	Eliminación o ajuste de los derechos de acceso
9.3		Responsabilidades del usuario
9.3.1	5.17	Uso de información de autenticación secreta
9.4		Control de acceso a sistemas y aplicaciones
9.4.1	8.3	Restricción de acceso a la información
9.4.2	8.5	Procedimientos seguros de inicio de sesión
9.4.3	5.17	Sistema de gestión de contraseñas
9.4.4	8.18	Uso de programas de utilidad privilegiados
9.4.5	8.4	Control de acceso al código fuente del programa
10		Criptografía
10.1		Controles criptográficos
10.1.1	8.24	Política sobre el uso de controles criptográficos
10.1.2	8.24	Gestión de claves

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002	Nombre de control según ISO/IEC 27002:2013
11		Seguridad física y ambiental
11.1		Áreas seguras
11.1.1	7.1	Perímetro de seguridad física
11.1.2	7.2	Controles de entrada física
11.1.3	7.3	Asegurar oficinas, salas e instalaciones
11.1.4	7.5	Protección contra amenazas externas y ambientales.
11.1.5	7.6	Trabajar en áreas seguras
11.1.6	7.2	Zonas de entrega y carga
11.2		Equipo
11.2.1	7.8	Emplazamiento y protección de equipos
11.2.2	7.11	Servicios de suministros
11.2.3	7.12	Seguridad del cableado
11.2.4	7.13	Mantenimiento de equipo
11.2.5	7.10	Eliminación de activos
11.2.6	7.9	Seguridad de equipos y activos fuera de las instalaciones
11.2.7	7.14	Eliminación segura o reutilización de equipos
11.2.8	8.1	Equipo de usuario desatendido
11.2.9	7.7	Política de escritorio y pantalla limpios
12		Seguridad de las operaciones
12.1		Procedimientos operativos y responsabilidades
12.1.1	5.37	Procedimientos operativos documentados
12.1.2	8.32	Gestión del cambio
12.1.3	8.6	Gestión de capacidad
12.1.4	8.31	Separación de entornos de desarrollo, pruebas y operativos
12.2		Protección contra software malicioso
12.2.1	8.7	Controles contra software malicioso
12.3		Respaldo
12.3.1	8.13	Respaldo de la información
12.4		Registro y monitoreo
12.4.1	8.15	El registro de eventos
12.4.2	8.15	Protección de la información de registro
12.4.3	8.15	Registros de administrador y operador
12.4.4	8.17	Sincronización de reloj
12.5		Control de software operativo
12.5.1	8.19	Instalación de software en sistemas operativos
12.6		Gestión de vulnerabilidades técnicas
12.6.1	8.8	Gestión de vulnerabilidades técnicas
12.6.2	8.19	Restricciones en la instalación de software
12.7		Consideraciones de auditoría de sistemas de información
12.7.1	8.34	Controles de auditoría de sistemas de información

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002	Nombre de control según ISO/IEC 27002:2013
13		Seguridad de las comunicaciones
13.1		Instalaciones de gestión de seguridad de red.
13.1.1	8.20	Controles de red
13.1.2	8.21	Seguridad de los servicios de red.
13.1.3	8.22	Segregación en redes
13.2		Transferencia de información
13.2.1	5.14	Políticas y procedimientos de transferencia de información
13.2.2	5.14	Acuerdos de transferencia de información
13.2.3	5.14	Mensajería electrónica
13.2.4	6.6	Acuerdos de confidencialidad o no divulgación
14		Adquisición, desarrollo y mantenimiento del sistema
14.1		Requisitos de seguridad de los sistemas de información
14.1.1	5.8	Análisis y especificación de requisitos de seguridad de la información.
14.1.2	8.26	Protección de servicios de aplicaciones en redes públicas
14.1.3	8.26	Protección de transacciones de servicios de aplicaciones
14.2		Seguridad en los procesos de desarrollo y soporte
14.2.1	8.25	Política de desarrollo seguro
14.2.2	8.32	Procedimientos de control de cambios del sistema
14.2.3	8.32	Revisión técnica de aplicaciones tras cambios de plataforma operativa
14.2.4	8.32	Restricciones a los cambios en los paquetes de software
14.2.5	8.27	Principios de ingeniería de sistemas seguros
14.2.6	8.31	Entorno de desarrollo seguro
14.2.7	8.30	Desarrollo subcontratado
14.2.8	8.29	Pruebas de seguridad del sistema
14.2.9	8.29	Pruebas de aceptación del sistema
14.3		Datos de prueba
14.3.1	8.33	Protección de datos de prueba
15		Relaciones con proveedores
15.1		Seguridad de la información en las relaciones con los proveedores
15.1.1	5.19	Política de seguridad de la información en las relaciones con proveedores
15.1.2	5.20	Abordar la seguridad en los acuerdos con los proveedores
15.1.3	5.21	Cadena de suministro de tecnología de la información y la comunicación
15.2		Gestión de entrega de servicios de proveedores
15.2.1	5.22	Seguimiento y revisión de servicios de proveedores

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002	Nombre de control según ISO/IEC 27002:2013
15.2.2	5.22	Gestión de cambios en los servicios del proveedor
16		Gestión de incidentes de seguridad de la información
16.1		Gestión de incidentes y mejoras de seguridad de la información
16.1.1	5.24	Responsabilidades y procedimientos
16.1.2	6.8	Reportar eventos de seguridad de la información
16.1.3	6.8	Informar sobre debilidades en la seguridad de la información
16.1.4	5.25	Evaluación y decisión sobre eventos de seguridad de la información
16.1.5	5.26	Respuesta a incidentes de seguridad de la información
16.1.6	5.27	Aprender de los incidentes de seguridad de la información
16.1.7	5.28	Recolección de evidencia
17		Aspectos de seguridad de la información de la gestión de la continuidad del negocio
17.1		Continuidad de la seguridad de la información
17.1.1	5.29	Planificación de la continuidad de la seguridad de la información
17.1.2	5.29	Implementación de la continuidad de la seguridad de la información
17.1.3	5.29	Verificar, revisar y evaluar la continuidad de la seguridad de la información
17.2		Redundancias
17.2.1	8.14	Disponibilidad de instalaciones de procesamiento de información
18		Cumplimiento
18.1		Cumplimiento de requisitos legales y contractuales
18.1.1	5.31	Identificación de la legislación aplicable y requisitos contractuales
18.1.2	5.32	Derechos de propiedad intelectual
18.1.3	5.33	Protección de registros
18.1.4	5.34	Privacidad y protección de la información de identificación personal
18.1.5	5.31	Regulación de controles criptográficos
18.2		Revisiones de seguridad de la información
18.2.1	5.35	Revisión independiente de la seguridad de la información.
18.2.2	5.36	Cumplimiento de políticas y estándares de seguridad
18.2.3	5.36, 8.8	Revisión de cumplimiento técnico

BIBLIOGRAFÍA

[1] ISO 9000, *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:—[2)], *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*

[2)] Bajo preparación. Etapa en el momento de la publicación: ISO/IEC PRF 23751:2022.

[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