Norma Española

UNE-EN ISO/IEC 27002

Mayo 2023

Versión corregida, junio 2023

Seguridad de la información, ciberseguridad y protección de la privacidad

Control de la seguridad de la información

(ISO/IEC 27002:2022)

Esta norma ha sido elaborada por el comité técnico CTN-UNE 320 *Ciberseguridad y protección de datos personales*, cuya secretaría desempeña UNE.

Asociación Española de Normalización

Calle de Génova, 6
28004 Madrid. España

915 294 900
info@une.org – www.une.org

UNE-EN ISO/IEC 27002

Seguridad de la información, ciberseguridad y protección de la privacidad Control de la seguridad de la información (ISO/IEC 27002:2022)

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

Sécurité de l'information, cybersécurité et protection de la vie privée. Moyens de maîtrise de l'information (ISO/IEC 27002:2022).

Esta norma es la versión oficial, en español, de la Norma Europea EN ISO/IEC 27002:2022, que a su vez adopta la Norma Internacional ISO/IEC 27002:2022.

Esta norma anula y sustituye a la Norma UNE-EN ISO/IEC 27002:2017.

Esta versión corregida de la Norma UNE-EN ISO/IEC 27002:2023 incorpora las siguientes correcciones:

- Se modifican los encabezados de las tablas B.1 y B.2.
- Se añade un párrafo entre las tablas B.1 y B.2.

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

UNE

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27002

Noviembre 2022

ICS 35.030

Sustituye a EN ISO/IEC 27002:2017

Versión en español

Seguridad de la información, ciberseguridad y protección de la privacidad Control de la seguridad de la información (ISO/IEC 27002:2022)

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

Sécurité de l'information, cybersécurité et protection de la vie privée. Moyens de maîtrise de l'information (ISO/IEC 27002:2022).

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre. Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022).

Esta norma europea ha sido aprobada por CEN/CENELEC el 2022-10-30.

Los miembros de CEN/CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional. Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales pueden obtenerse en el Centro de Gestión de CEN/CENELEC, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CEN/CENELEC en su idioma nacional, y notificada al Centro de Gestión de CEN/CENELEC, tiene el mismo rango que aquéllas.

Los miembros de CEN/CENELEC son los organismos nacionales de normalización y los comités electrotécnicos nacionales de los países siguientes: Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República de Macedonia del Norte, Rumanía, Serbia, Suecia, Suiza y Turquía.

CENTRO DE GESTIÓN DE CEN/CENELEC
Rue de la Science, 23, B-1040 Brussels, Belgium

Índice

Prólogo europeo

El texto de la Norma ISO/IEC 27002:2022 del Comité Técnico ISO/IEC JTC 1 *Tecnología de la información*, de la Organización Internacional de Normalización (ISO), ha sido adoptado como Norma EN ISO/IEC 27002:2022 por el Comité Técnico CEN-CENELEC/JTC 13 *Ciberseguridad y protección de datos*, cuya Secretaría desempeña DIN.

Esta norma europea debe recibir el rango de norma nacional mediante la publicación de un texto idéntico a ella o mediante ratificación antes de finales de mayo de 2023, y todas las normas nacionales técnicamente divergentes deben anularse antes de finales de mayo de 2023.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN y/o CENELEC no son responsables de la identificación de dichos derechos de patente.

Esta norma anula y sustituye a la Norma EN ISO/IEC 27002:2017.

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En la web de CEN y CENELEC se puede encontrar un listado completo de estos organismos.

De acuerdo con el Reglamento Interior de CEN/CENELEC, están obligados a adoptar esta norma europea los organismos de normalización de los siguientes países: Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República de Macedonia del Norte, Rumanía, Serbia, Suecia, Suiza y Turquía.

Declaración

El texto de la Norma ISO/IEC 27002:2022 ha sido aprobado por CEN/CENELEC como Norma EN ISO/IEC 27002:2022 sin ninguna modificación.

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de elaboración de las Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, vinculadas con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los temas de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y aquellos previstos para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento ha sido redactado de acuerdo con las reglas editoriales de la Parte 2 de las Directivas ISO/IEC (véase www.iso.org/directives o www.iec.ch/members_experts/refdocs).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de alguno o todos los derechos de patente. Los detalles sobre cualquier derecho de patente identificado durante el desarrollo de este documento se indicarán en la Introducción y/o en la lista ISO de declaraciones de patente recibidas (véase www.iso.org/patents) o en la lista IEC (véase https://patents.iec.ch/).

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos específicos de ISO y las expresiones relacionadas con la evaluación de la conformidad, así como la información acerca de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html. En la 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. A su vez, incorpora los Corregindum Técnicos ISO/IEC 27002:2013/Cor. 1:2014 y ISO/IEC 27002:2013/Cor. 2:2015.

Los cambios principales en comparación con la edición previa son los siguientes:

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

En la actual versión corregida de ISO/IEC 27002:2022 se incorporan las siguientes correcciones:

– se han restaurado los hipervínculos que no funcionaban en el documento;

– en la tabla introductoria del apartado 5.22 y en la tabla A.1 (fila 5.22), "#Garantías de seguridad de la información" se ha trasladado de la columna titulada "Dominios de seguridad" a la columna titulada "Capacidades operativas".

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En www.iso.org/members.html y https://www.iec.ch/national-committees se puede encontrar un listado completo de estos organismos.

0 Introducción

0.1 Antecedentes y contexto

Este documento está destinado a organizaciones de todo tipo y tamaño. Se debe utilizar como referencia para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información en un sistema de gestión de seguridad de la información (SGSI) basado en la Norma ISO/IEC 27001. También puede utilizarse como documento de orientación para las organizaciones que determinan e implementan controles de seguridad de la información comúnmente aceptados. Además, este documento está pensado también para usarse en el desarrollo de directrices de gestión de la seguridad de la información en industrias y organizaciones específicas, teniendo en cuenta su(s) entorno(s) de riesgo de seguridad de la información específico(s). Los controles específicos de la organización o del entorno distintos a los incluidos en este documento pueden determinarse mediante la evaluación de riesgos, según sea necesario.

Organizaciones de todo tipo y tamaño (del sector público y privado, comerciales y sin ánimo de lucro) crean, recopilan, procesan, almacenan, transmiten y eliminan información en muchas formas, incluidas la electrónica, la física y la verbal (por ejemplo, conversaciones y presentaciones).

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

La seguridad de la información se consigue implementando un conjunto adecuado de controles, entre los que se incluyen políticas, normas, procesos, procedimientos, estructuras organizativas y funciones de *software* y *hardware*. Para cumplir sus objetivos específicos de seguridad y de negocio, la organización debería definir, implementarse, supervisar, revisar y mejorar estos controles cuando sea necesario. Un SGSI como el especificado en la Norma ISO/IEC 27001 adopta una visión holística y coordinada de los riesgos de seguridad de la información de la organización con el fin de determinar e implementar un conjunto completo de controles de seguridad de la información dentro del marco general de un sistema de gestión coherente.

Muchos sistemas de información, incluyendo su gestión y operaciones, no han sido diseñados para ser seguros en términos de un SGSI tal y como se especifica en la Norma ISO/IEC 27001 y en este documento. El nivel de seguridad que puede lograrse sólo a través de medidas tecnológicas es limitado y debería ser apoyado por actividades de gestión y procesos organizativos adecuados. La identificación de los controles que debería aplicarse requiere una planificación cuidadosa y atención a los detalles mientras se lleva a cabo el tratamiento de riesgos.

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

Un SGSI apropiado, adecuado y eficaz garantiza a la dirección de la organización y a otras partes interesadas que su información y otros activos asociados se mantienen razonablemente seguros y protegidos frente a amenazas y daños, permitiendo así 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. Existen tres fuentes principales de requisitos de seguridad de la información:

a) la evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos de negocio globales de la organización. Esto puede facilitarse o apoyarse mediante una evaluación de riesgos específica de la seguridad de la información. El resultado debería ser la determinación de los controles necesarios para garantizar que el riesgo residual para la organización cumple sus criterios de aceptación del riesgo;

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

c) el conjunto de principios, objetivos y requisitos de negocio para todas las etapas del ciclo de vida de la información que una organización ha desarrollado para apoyar sus operaciones.

0.3 Controles

Un control se define como una medida que modifica o contiene el riesgo. Algunos de los controles de este documento son controles que modifican el riesgo, mientras que otros lo contienen. Una política de seguridad de la información, por ejemplo, sólo puede contener el riesgo, mientras que el cumplimiento de la política de seguridad de la información puede modificar el riesgo. Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo. Este documento proporciona una variedad de controles de seguridad de la información organizativos, humanos, físicos y tecnológicos derivados de las mejores prácticas reconocidas internacionalmente.

0.4 Determinar los controles

La determinación de los controles depende de las decisiones de la organización tras una evaluación de los riesgos, con un alcance claramente definido. Las decisiones relacionadas con los riesgos identificados deberían basarse en los criterios de aceptación de los riesgos, las opciones de tratamiento de riesgos y el enfoque de gestión de riesgos aplicado por la organización. La determinación de los controles también debería tener en consideración toda la legislación y reglamentación nacionales e internacionales pertinentes. La determinación de los controles también depende de la forma en que estos interactúan entre sí para proporcionar una defensa en profundidad.

La organización puede diseñar controles según sus necesidades o identificarlos a partir de 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. Véase el Informe ISO/IEC TR 27016 para obtener orientación sobre las decisiones relativas a la inversión en un SGSI y las consecuencias económicas de estas decisiones en el contexto de la competencia por los recursos.

Debería existir un equilibrio entre los recursos desplegados para implementar los controles y el impacto empresarial potencial resultante de los incidentes de seguridad en ausencia de dichos controles. Los resultados de una evaluación de riesgos deberían ayudar a orientar y determinar las medidas de gestión apropiadas, las prioridades para la gestión de los riesgos de seguridad de la información y para la aplicación de los controles que se determinen necesarios para proteger contra estos riesgos.

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

0.5 Elaboración de directrices específicas para cada organización

Este documento puede considerarse un punto de partida para desarrollar directrices específicas para cada organización. No todos los controles y directrices de este documento pueden ser aplicables a todas las organizaciones. También pueden ser necesarios controles y directrices adicionales no incluidos en este documento para abordar las necesidades específicas de la organización y los riesgos que se hayan identificado. Cuando se elaboren documentos que contengan directrices o controles adicionales, puede ser útil incluir referencias cruzadas a las cláusulas de este documento para futuras consultas.

0.6 Consideraciones relativas al ciclo de la vida

La información tiene un ciclo de vida, desde su creación hasta su eliminación. El valor de la información y los riesgos que corre 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 son significativos una vez han sido publicadas, pero la integridad sigue siendo fundamental), por lo que la seguridad de la información sigue siendo importante en cierta medida en todas las etapas.

Los sistemas de información y otros activos relevantes para la seguridad de la información tienen ciclos de vida dentro de los cuales se conciben, especifican, diseñan, desarrollan, prueban, implantan, utilizan, mantienen y finalmente se retiran del servicio y se eliminan. La seguridad de la información debería ser considerada en cada fase. Los proyectos de desarrollo de nuevos sistemas y los cambios en los sistemas existentes proporcionan oportunidades para mejorar los controles de seguridad teniendo en cuenta los riesgos de la organización y las lecciones aprendidas de los incidentes.

0.7 Normas internacionales relacionadas

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

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

Existen normas sectoriales específicas que disponen de controles adicionales cuyo objetivo es abordar ámbitos específicos (por ejemplo, la Norma ISO/IEC 27017 para los servicios en la nube, la Norma ISO/IEC 27701 para la privacidad, la Norma ISO/IEC 27019 para la energía, la Norma ISO/IEC 27011 para las organizaciones de telecomunicaciones y la Norma ISO 27799 para la salud). Estas normas se incluyen en la bibliografía y algunas de ellas se mencionan en las secciones de orientación y otra información de los capítulos 5 a 8.

1 Objeto y campo de aplicación

Este documento proporciona un conjunto de referencia de controles genéricos de seguridad de la información que incluyen orientaciones para su aplicación. Este documento está diseñado para ser utilizado por las organizaciones:

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

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

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

2 Normas para consulta

En este documento no hay normas para consulta.

3 Términos, definiciones y abreviaturas

3.1 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones siguientes:

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

– Plataforma de búsqueda en línea de ISO: disponible en http://www.iso.org/obp

– Electropedia de IEC: disponible en http://www.electropedia.org/

3.1.1 control de acceso:
Medios para garantizar que el acceso físico y lógico a los *activos* (3.1.2) está autorizado y restringido en función de los requisitos de seguridad de la empresa y de la información.

3.1.2 activo:
Cualquier cosa que tenga valor para la organización.

NOTA 1 En el contexto de la seguridad de la información, pueden distinguirse dos tipos de activos:

- los activos primarios:
  - la información;
  - los *procesos* de negocio (3.1.27) y las actividades;
- los activos de apoyo (de los que dependen los activos primarios) de todo tipo, por ejemplo:
  - *hardware*;
  - *software*;
  - redes;
  - *personal* (3.1.20);
  - emplazamiento;
  - estructura de la organización.

3.1.3 ataque:
Intento no autorizado, con o sin éxito, de destruir, alterar, inutilizar o acceder a un *activo* (3.1.2) o cualquier intento de exponer, robar o hacer un uso no autorizado de un *activo* (3.1.2).

3.1.4 autenticación:
Aportación de garantías de que son correctas las características que una *entidad* (3.1.11) reivindica para sí misma es correcta.

3.1.5 autenticidad:
Propiedad consistente en que una *entidad* (3.1.11) es lo que dice ser.

3.1.6 cadena de custodia:
Posesión, movimiento, manipulación y localización de material demostrables desde un momento hasta otro.

NOTA 1 El material incluye la información y otros *activos* asociados (3.1.2) en el contexto de la Norma ISO/IEC 27002.

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

3.1.7 Información confidencial:
Información que no se pretende poner a disposición o revelar a otras personas, *entidades* (3.1.11) o *procesos* (3.1.27).

3.1.8 control:
Medida que contiene y/o modifica un riesgo.

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

NOTA 2 Es posible que los controles no siempre ejerzan el efecto modificador previsto o supuesto.

[FUENTE: ISO 31000:2018, 3.8]

3.1.9 interrupción:
Incidente, previsto o imprevisto, que provoca una desviación negativa y no planificada de la entrega prevista de productos y servicios de acuerdo con los objetivos de una organización.

[FUENTE: ISO 22301:2019, 3.10]

3.1.10 dispositivo final:
Dispositivo *hardware* de tecnologías de la información y la comunicación (TIC) conectado a la red.

NOTA 1 Dispositivo final puede referirse a ordenadores de sobremesa, portátiles, teléfonos inteligentes, tabletas, clientes ligeros, impresoras u otro *hardware* especializado, incluidos contadores inteligentes y dispositivos del Internet de las cosas (IoT).

3.1.11 entidad:
Elemento relevante a efectos del funcionamiento de un dominio que tiene una existencia reconociblemente distinta.

NOTA 1 Una entidad puede tener una encarnación física o lógica.

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

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

3.1.12 instalación de tratamiento de información:
Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan.

[FUENTE: ISO/IEC 27000:2018, 3.27, modificado - "instalaciones" se ha sustituido por “instalación”].

3.1.13 brecha en la seguridad de la información:
Compromiso de la seguridad de la información que provoca la destrucción, pérdida, alteración, divulgación o acceso no deseados a información protegida transmitida, almacenada o procesada de otro modo, o el acceso a información protegida transmitida, almacenada o tratada de otro modo.

3.1.14 evento de seguridad de la información:
Ocurrencia que indica una posible *brecha en la seguridad de la información* (3.1.13) o un fallo de los *controles* (3.1.8).

[FUENTE: ISO/IEC 27035-1:2016, 3.3, modificado - "violación de la seguridad de la información" se ha sustituido por "brecha en la seguridad de la información"].

3.1.15 incidente de seguridad de la información:
Evento singular o serie de *eventos de seguridad de la información* (3.1.14), inesperados o no deseados, que tienen la posibilidad de dañar los *activos* de una organización (3.1.2) o comprometer sus *operaciones* (3.1.13).

[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 la gestión 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 tecnologías de la información u otros componentes que manejan información.

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

3.1.18 parte interesada:
Persona u organización que puede afectar, estar afectada o percibir que está afectada por una decisión o actividad.

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

3.1.19 no repudio:
Capacidad para corroborar la reivindicación de la ocurrencia de un evento o acción por parte de las *entidades* (3.1.11) que lo originaron.

3.1.20 personal:
Personas que realizan un trabajo bajo la dirección de la organización.

NOTA 1 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 personal identificable (PII):
Cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o (b) esté o pueda estar directa o indirectamente vinculada a una persona física.

NOTA 1 La "persona física" en la definición es el *titular de la PII* (3.1.22). Para determinar si un interesado es identificable, deberían tenerse en cuenta todos los medios que puedan ser razonablemente utilizados por la parte interesada que posea los datos, o por cualquier otra parte, para establecer el vínculo entre el conjunto de PII y la persona física.

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

3.1.22 titular de la PII:
Persona física a la que se refiere la *información personal identificable (PII)* (3.1.21).

NOTA 1 Dependiendo de la jurisdicción y de la legislación particular sobre protección de datos y privacidad, también puede utilizarse el sinónimo "interesado" en lugar del término "titular de la PII".

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

3.1.23 encargado del Tratamiento:
Parte interesada que trata *información personal identificable (PII)* (3.1.21) en nombre y de acuerdo con las instrucciones de un Responsable del Tratamiento de la PII.

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

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

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

3.1.25 evaluación de impacto relativa a protección de datos (EIPD):
Proceso (3.1.27) global de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de los posibles impactos sobre la privacidad en relación con el tratamiento de *información personal identificable (PII)* (3.1.21), enmarcado en un marco más amplio de gestión de riesgos de una organización.

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

3.1.26 procedimiento:
Forma especificada de llevar a cabo una actividad o un *proceso* (3.1.27).

[FUENTE: ISO 30000:2009, 3.12]

3.1.27 proceso:
Conjunto de actividades interrelacionadas o que interactúan entre sí y que utilizan o transforman elementos de entrada para producir un resultado.

[FUENTE: ISO 9000:2015, 3.4.1, modificado- Notas a la entrada eliminadas].

3.1.28 registro:
Información creada, recibida y conservada como prueba 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 Las obligaciones legales en este contexto incluyen todos los requisitos legales, estatutarios, reglamentarios y contractuales.

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

3.1.29 objetivo de Punto de Recuperación (RPO):
Punto en el tiempo en el que deben ser recuperados los datos después de que se haya producido una *interrupción* (3.1.9).

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

3.1.30 objetivo de Tiempo de Recuperación (RTO):
Periodo de tiempo en el que deben ser recuperados los niveles mínimos de servicios y/o productos y los sistemas de soporte, aplicaciones o funciones tras una *interrupción* (3.1.9).

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

3.1.31 fiabilidad:
Propiedad de que la consistencia en el comportamiento y los resultados previstos sean coherentes.

3.1.32 regla:
Principio o instrucción aceptada que establece las expectativas de la organización sobre lo que se debe hacer, lo que está permitido o lo que no.

NOTA 1 Las reglas pueden expresarse formalmente en *políticas específicas* (3.1.35) y en otros tipos de documentos.

3.1.33 información sensible:
Información que debe ser protegida frente a la indisponibilidad, el acceso no autorizado, la modificación o la divulgación pública, debido a posibles efectos adversos sobre una persona, organización, seguridad nacional o seguridad pública.

3.1.34 amenaza:
Causa potencial de un incidente no deseado, que puede provocar daños en un sistema u organización.

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

3.1.35 política específica:
Intenciones y orientaciones sobre un asunto o tema específico, expresadas formalmente por el nivel de dirección adecuado.

NOTA 1 Las políticas específicas pueden expresar formalmente *reglas* (3.1.32) o normas de la organización.

NOTA 2 Algunas organizaciones utilizan otros términos para referirse a estas políticas específicas.

NOTA 3 Las políticas específicas a las que se hace referencia en este documento están relacionadas con la seguridad de la información.

EJEMPLO Política específica de *control de acceso* (3.1.1), política específica puesto de trabajo despejado y pantalla limpia.

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, proveedores.

3.1.37 dispositivo final de usuario:
Dispositivo finall (3.1.10) utilizado por los usuarios para acceder a los servicios de tratamiento de la información.

NOTA 1 Dispositivo final de usuario puede referirse a ordenadores de sobremesa, portátiles, teléfonos inteligentes, tabletas, clientes ligeros, etc.

3.1.38 vulnerabilidad:
Debilidad de un *activo* (3.1.2) o *control* (3.1.8) que puede ser explotada por una o más *amenazas* (3.1.34).

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

3.2 Términos abreviados

ABAC	control de acceso basado en atributos
ACL	lista de control de acceso
BIA	análisis de impacto del negocio
BYOD	trae tu propio dispositivo
CAPTCHA	prueba de Turing público y automático para distinguir a los ordenadores de los humanos
CPU	unidad central de procesamiento
DAC	control de acceso discrecional
DNS	sistema de nombres de dominio
EIPD	evaluación de impacto relativa a la protección de datos
GPS	sistema de posicionamiento global
IAM	gestión de identidad de acceso
ID	identificador

IDE	entorno de desarrollo integrado
IDS	sistema de detección de intrusos
PII	información de identificación personal
Iot	internet de las cosas
IP	protocolo de internet
IPS	sistema de prevención de intrusos
IT	tecnología de la información
MAC	control de acceso obligatorio
NTP	protocolo de tiempo de red
PIN	número de identificación personal
PKI	infraestructura de clave pública
PTP	protocolo de tiempo de precisión
RBAC	control de acceso basado en roles
RPO	objetivo de punto de recuperación
RTO	objetivo de tiempo de recuperación
SAI	sistema de alimentación ininterrumpida
SAST	pruebas de seguridad de aplicaciones estáticas
SD	seguridad digital
SDN	redes definidas por *Software*
SD-WAN	red de área extensa definida por *Software*
SGSI	sistema de gestión de seguridad de la información
SIEM	gestión de eventos e información de seguridad
SMS	servicio de mensajes cortos
SQL	lenguaje de consulta estructurada
SSO	inicio de sesión único
SWID	etiquetas de identificación de *Software*
TIC	tecnologías de la información y la comunicación
UEBA	análisis de comportamiento de los usuarios y entidades
URL	identificador de recursos uniforme

USB	bus universal en serie
VM	máquina virtual
VPN	red privada virtual
WiFi	fibra inalámbrica

4 Estructura del documento

4.1 Capítulos

Este documento está estructurado de la siguiente manera.

a) Controles organizativos (capítulo 5)

b) Controles de personas (capítulo 6)

c) Controles físicos (capítulo 7)

d) Controles tecnológicos (capítulo 8)

Hay 2 anexos informativos:

– Anexo A: Uso de atributos

– Anexo B: Correspondencia con la Norma ISO/IEC 27002:2013

El anexo A explica cómo una organización puede utilizar atributos (véase 4.2) para crear sus propias visualizaciones, basadas en los atributos de los controles definidos en este documento o los de su propia creación.

El anexo B muestra la correspondencia entre los controles de la presente edición de la Norma ISO/IEC 27002 y la edición anterior de 2013.

4.2 Temas y atributos

La clasificación de los controles que aparecen en los capítulos 5 a 8 se conocen como temas.

Los controles se clasifican como:

a) personas, si se refieren a personas individuales;

b) físicos, si se refieren a objetos físicos;

c) tecnológicos, si afectan a la tecnología;

d) de lo contrario, se clasifican como organizativos.

La organización puede utilizar atributos para crear diferentes visualizaciones, que son diferentes categorizaciones de los controles vistos desde una perspectiva diferente a los temas. Los atributos pueden utilizarse para filtrar, clasificar o presentar los controles en diferentes puntos de vista para diferentes audiencias. El anexo A explica cómo se puede lograr esto y proporciona un ejemplo de una visualización.

A modo de ejemplo, cada control de este documento se ha asociado a cinco atributos con sus correspondientes valores de atributo (precedidos de "#" para que se puedan buscar), como se indica a continuación:

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 del atributo consisten en Preventivo (el control que pretende evitar la ocurrencia de un incidente de seguridad de la información), Detectivo (el control actúa cuando se produce un incidente de seguridad de la información) y Correctivo (el control actúa después de que se produzca un incidente de seguridad de la información).

b) Dimensiones de seguridad de la información

Las dimensiones de seguridad de la información son un atributo para ver los controles desde la perspectiva de qué características de la información contribuirá a preservar. Los valores del atributo son Confidencialidad, Integridad y Disponibilidad.

c) Conceptos de ciberseguridad

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

d) Capacidades operativas

Las capacidades operativas son un atributo para ver los controles desde la perspectiva del profesional de las capacidades de seguridad de la información. Los valores del atributo consisten en Gobernanza, Gestión de activos, Protección de la información, Seguridad de los recursos humanos, Seguridad física, Seguridad de los sistemas y de las redes, Seguridad de las aplicaciones, Configuración segura, Gestión de la identidad y del acceso, Gestión de las amenazas y de la vulnerabilidad, Continuidad, Seguridad de las relaciones con los proveedores, Legalidad y Cumplimiento normativo, Gestión de eventos de seguridad de la información y Garantía de 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 de los sistemas de información y gestión de riesgos" y "Gestión de la ciberseguridad del ecosistema" (incluidas las partes interesadas internas y externas); "Protección" incluye "Arquitectura de la seguridad informática", "Administración de la seguridad informática", "Gestión de la identidad y el acceso", "Mantenimiento de la seguridad informática" y "Seguridad física y del entorno"; "Defensa" incluye "Detección" y "Gestión de incidentes de seguridad informática"; "Resiliencia" incluye "Continuidad de las operaciones" y "Gestión de crisis". Los valores de los atributos consisten en "Gobernanza y ecosistema", "Protección", "Defensa" y "Resiliencia".

Los atributos que figuran en este documento se han seleccionado porque se consideran lo suficientemente genéricos como para ser utilizados por distintos tipos de organizaciones. Las organizaciones pueden optar por hacer caso omiso de uno o varios de los atributos que figuran en este documento. También pueden crear atributos propios (con los valores de atributo correspondientes) para crear sus propias visualizaciones organizativas. El capítulo A.2 incluye ejemplos de tales atributos.

4.3 Panel de control

El esquema de cada control contiene lo siguiente:

- **título del control:** Nombre corto del control;
- **tabla de atributos:** Una tabla muestra el valor o valores de cada atributo para el control dado;
- **control:** Qué control es;
- **propósito:** Por qué debería implementarse el control;
- **orientación:** Cómo debería implementarse el control;
- **información adicional:** Texto explicativo o referencias a otros documentos relacionados.

En el texto de algunas orientaciones se utilizan subtítulos para facilitar la lectura cuando las orientaciones son extensas y abordan varios temas. No se utilizan necesariamente en todo el texto de orientación. Los subtítulos aparecen subrayados.

5 Organización

5.1 Políticas para la seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_Ecosistema #Resiliencia

Control

La política de seguridad de la información y un conjunto de políticas específicas deberían ser definidas, aprobadas por la dirección, publicadas, comunicadas y conocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.

Propósito

Garantizar la continua idoneidad, adecuación, efectividad de la dirección y apoyo a la seguridad de la información de acuerdo con los requisitos de negocio, legales, estatutarios, reglamentarios y contractuales.

Orientación

La organización debería definir una "política de seguridad de la información" al máximo nivel que sea aprobada por la alta dirección y que establezca el enfoque de la organización para gestionar la seguridad de la información.

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

a) la estrategia y requisitos de negocio;

b) la normativa, legislación y contratos;

c) el entorno actual y previsto de riesgos y amenazas para la seguridad de la información.

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

a) la definición de la seguridad de la información;

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

c) los principios para orientar todas las actividades concernientes a la seguridad de la información;

d) el compromiso de satisfacer los requisitos aplicables concernientes a la seguridad de la información;

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

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

g) los procedimientos para el tratamiento de exenciones y excepciones.

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

A un nivel inferior, la política de seguridad de la información debería apoyarse en políticas específicas, según sea necesario, para profundizar en la implementación de los controles de seguridad de la información. Las políticas específicas, por lo general, están estructuradas para atender las necesidades de determinados grupos dentro de una organización o para cubrir ciertas áreas de seguridad. Las políticas específicas deberían estar alineadas y complementar la política de seguridad de la información de la organización.

Ejemplos de estas temáticas incluyen:

a) control de acceso;

b) seguridad física y ambiental;

c) gestión de activos;

d) transferencia de información;

e) configuración y tratamiento seguros de los dispositivos finales de los usuarios;

f) seguridad de la red;

g) gestión de incidentes de seguridad de la información;

h) copias de respaldo;

i) criptografía y gestión de claves;

j) clasificación y tratamiento de la información;

k) gestión de las vulnerabilidades técnicas;

l) desarrollo seguro.

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

a) la estrategia de negocio de la organización;

b) el entorno técnico de la organización;

c) la normativa, estatutos, legislación y contratos;

d) los riesgos para la seguridad de la información;

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

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

La revisión de la política de seguridad de la información y de las políticas específicas debería tener en consideración los resultados de las revisiones y auditorías realizadas por la dirección. Debería considerarse la revisión y actualización de otras políticas relacionadas cuando se modifique una política para mantener la coherencia.

La política de seguridad de la información y las políticas específicas deberían ser comunicadas al personal relevante y partes interesadas de una forma que sea apropiada, accesible y comprensible para el lector al que va dirigida. A los destinatarios de las políticas se les debería exigir que reconozcan que las entienden y que se comprometen a cumplirlas, cuando corresponda. La organización puede determinar el formato y denominación de estos documentos normativos de acuerdo con las necesidades de la organización. En algunas organizaciones, la política de seguridad de la información y las políticas específicas pueden recogerse en un solo documento. La organización puede denominar estas políticas específicas por temas como normas, directivas, políticas u otros. La organización puede denominar estas políticas específicas como normas, directivas, políticas u otros.

Si la política de seguridad de la información o cualquier política específicas es distribuida al exterior de la organización, se debería tener cuidado de no revelar incorrectamente información confidencial.

La tabla 1 muestra las diferencias entre la política de seguridad de la información y la política específica.

Table 1 – Diferencias entre la política de seguridad de la información y la política específica

	Política de seguridad de la información	**Política específica**
Nivel de detalle	General o de nivel alto	Específica y detallada
Documentada y aprobada formalmente por	Alta dirección	Nivel de dirección adecuado

Información adicional

Las políticas específicas pueden variar según las organizaciones.

5.2 Roles y responsabilidades en seguridad de la información

Tipo de control	**Dimensiones de seguridad de la información**	**Conceptos de ciberseguridad**	**Capacidades operativas**	**Dominios de seguridad**
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_Ecosistema #Protección #Resiliencia

Control

Todos 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 comprensible para la implementación, operación y gestión de la seguridad de la información dentro de la organización.

Orientación

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

a) proteger la información y otros activos asociados;

b) realizar procesos específicos de seguridad de la información;

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

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

Estas responsabilidades deberían completarse, cuando sea necesario, con una guía más detallada para ubicaciones e instalaciones de tratamiento de la información específicas. Las personas con responsabilidades asignadas en materia de seguridad de la información pueden asignar tareas de seguridad a otras personas. Sin embargo, siguen siendo responsables y deberían comprobar que las tareas delegadas se han realizado correctamente.

Cada área de seguridad de la que es una persona es responsable debería ser definida, documentada y comunicada. Los niveles de autorización deberían ser definidos y documentados. Las personas que asuman un rol específico en materia de seguridad de la información deberían ser competentes en los conocimientos y habilidades requeridos por el rol y deberían recibir apoyo para mantenerse al día con los desarrollos relacionados y necesarios para cumplir con las responsabilidades del mismo.

Información adicional

En muchas organizaciones se nombra un responsable de seguridad de la información para asumir la responsabilidad general del desarrollo e implantación de la seguridad de la información y para dar soporte a la identificación de los riesgos y los controles de mitigación.

Sin embargo, la responsabilidad de la provisión e implantación de los controles a menudo permanece en directivos a título individual. Una práctica común es nombrar un propietario para cada activo quien se hace responsable de la protección en el día a día.

Dependiendo del tamaño y de los recursos de una organización, la seguridad de la información puede ser cubierta mediante funciones o deberes adicionales a los ya existentes.

5.3 Segregación de tareas

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernanza #Gestión_de_identidad_acceso	#Gobernanza_y_Ecosistema

Control

Las funciones y áreas de responsabilidad en conflicto deberían segregarse.

Propósito

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

Orientación

La segregación de tareas y áreas de responsabilidad tiene como objetivo separar las tareas conflictivas entre diferentes personas para evitar que una persona ejecute por sí misma posibles deberes contradictorios.

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

a) iniciar, aprobar y ejecutar un cambio;

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

c) diseño, implementación y revisión de código;

d) desarrollo de *software* y administración de sistemas de producción;

e) uso y administración de aplicaciones;

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

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

La posibilidad de colusión debería ser tenida en cuenta al diseñar los controles de segregación. Las organizaciones pequeñas pueden considerar que la segregación de tareas es difícil de conseguir, pero el principio debería aplicarse en la medida en que sea posible y practicable. Cuando la segregación sea difícil, se deberían considerar otros controles como la monitorización de actividades, los registros de auditoría y la supervisión por la dirección.

Al utilizar sistemas de control de acceso basados en roles, se debería tener cuidado de que no se concedan a las personas roles conflictivos. Cuando hay un gran número de roles, la organización debería considerar el uso de herramientas automatizadas para identificar conflictos y facilitar su eliminación. Los roles deberían ser cuidadosamente definidos y aprovisionados para minimizar los problemas de acceso si un rol es eliminado o reasignado.

Información adicional

Ninguna información adicional.

5.4 Responsabilidades de la dirección

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_y_Ecosistema

Control

La dirección debería exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información, las políticas específicas y sus procedimientos específicos establecidos en la organización.

Propósito

Garantizar que la dirección comprenda su papel en la seguridad de la información y emprende acciones destinadas a asegurar que todo el personal conozca y cumpla con sus responsabilidades en seguridad de la información.

Orientación

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

Las responsabilidades de la dirección deberían garantizar que el personal:

a) este debidamente informado sobre sus roles y responsabilidades relativas a la seguridad de la información previamente a serles concedido el acceso a información de la organización y a otros activos asociados;

b) se les proporcionan directrices que establecen las expectativas en materia de seguridad de la información en lo relativo a su función dentro de la organización;

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

d) alcanzan un nivel de concienciación en seguridad de la información adecuado a sus funciones y responsabilidades dentro de la organización (véase 6.3);

e) cumple con los términos y condiciones de su contratación, incluyendo la política de seguridad de la información de la organización y los métodos de trabajo apropiados;

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

g) siempre que sea posible, disponen de un canal confidencial para denunciar las violaciones de la política de seguridad de la información, las políticas específicas o de los procedimientos de seguridad de la información *("whistleblowing"*). Esto puede permitir realizar denuncias anónimas, o tener disposiciones que garanticen que la identidad del denunciante sólo será conocida por aquellos que necesiten tratar dichos informes;

h) se les proporciona los recursos adecuados y el tiempo de planificación del proyecto para implementar los procesos y controles relacionados con la seguridad de la organización.

Información adicional

Ninguna información adicional.

5.5 Contacto con las autoridades

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resiliencia

Control

Deberían establecerse y mantenerse los contactos adecuados con las autoridades pertinentes.

Propósito

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

Orientación

La organización debería especificar cuándo y a qué autoridades se debería contactar (por ejemplo, cuerpos de seguridad, organismos reguladores, autoridades supervisoras) y cómo deberían ser notificados los incidentes de seguridad de la información identificados.

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

Información adicional

Las organizaciones que sufran un ataque pueden solicitar a las autoridades para emprender acciones contra la fuente del ataque.

Mantener tales contactos puede ser un requisito para dar soporte a la gestión de los incidentes de seguridad de la información (véase 5.24 a 5.28) o a la continuidad de negocio y a los planes de contingencia (véase 5.29 y 5.30). Los contactos con los organismos reguladores son también útiles para anticiparse y prepararse para los próximos cambios en las leyes o reglamentos pertinentes que afecten a la organización. Los contactos con otras autoridades incluyen a los servicios públicos, servicios de emergencia, proveedores de suministro eléctrico, de seguridad y de salud, (por ejemplo, cuerpos de bomberos (en relación a la continuidad de negocio), proveedores de servicios de telecomunicación (en relación con la disponibilidad y enrutamiento del servicio) y compañías de suministro de agua (en relación con las instalaciones de refrigeración para los equipos).

5.6 Contacto con grupos de interés especial

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

Control

Deberían establecerse y mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad.

Propósito

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

Orientación

La participación como miembro en grupos de interés especial o foros debería ser considerado como un medio para:

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

b) garantizar que un conocimiento actualizado del entorno de seguridad de la información;

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

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

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

f) proporcionar adecuados puntos de enlace relacionados con incidentes de seguridad de la información (véase 5.24 a 5.28).

Información adicional

Ninguna otra información.

5.7 Inteligencia de amenazas

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Amenazas_y_vulnerabilidades_de_la_dirección	#Defensa #Resiliencia

Control

La información relativa a las amenazas a la seguridad de la información debería recopilarse y analizarse para producir información sobre amenazas.

Propósito

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

Orientación

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

a) facilitar acciones fundamentadas para evitar que las amenazas causen daños a la organización;

b) reducir el impacto de dichas amenazas.

La inteligencia sobre amenazas puede dividirse en tres niveles, que deberían ser tenidos en cuenta:

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

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

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

La inteligencia sobre amenazas debería ser:

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

b) esclarecedora (es decir, que proporcione a la organización un conocimiento preciso y detallado del panorama de las amenazas);

c) contextual, para proporcionar un conocimiento de la situación (es decir, añadiendo un contexto a la información en base al momento de los hechos, el lugar donde ocurren, las experiencias previas y la prevalencia en organizaciones similares);

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

Las actividades de información sobre amenazas deberían incluir:

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

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

c) la recogida de información de las fuentes seleccionadas, que pueden ser internas y externas;

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

e) analizar la información para entender cómo se relaciona y su valor para la organización;

f) comunicarla y compartirla con las personas relevantes en un formato comprensible.

La inteligencia sobre amenazas debería ser analizada y posteriormente utilizada:

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

b) como aportación adicional a los controles técnicos preventivos y de detección, como cortafuegos, sistemas de detección de intrusos o soluciones contra el código dañino;

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

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

Información adicional

Las organizaciones pueden utilizar la inteligencia sobre amenazas para prevenir, detectar o responder a las mismas. Las organizaciones pueden producir inteligencia sobre amenazas, pero lo más habitual es que reciban y utilicen la inteligencia procedente de otras fuentes.

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

La eficacia de los controles, como el 5.25, el 8.7, el 8.16 o el 8.23, depende de la calidad de la inteligencia sobre amenazas disponible.

5.8 Seguridad de la información en la gestión de proyectos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gobernanza	#Gobernanza_y_Ecosistema #Protección

Control

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

Propósito

Garantizar que los riesgos de seguridad de la información relacionados con los proyectos y los resultados son abordados de forma eficaz en la gestión de proyectos a lo largo de todo su ciclo de vida.

Orientación

La seguridad de la información debería integrarse en la gestión de proyectos de la organización para garantizar que los riesgos de seguridad de la información sean contemplados en la gestión del proyecto. Esto es aplicable a cualquier tipo de proyecto, independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación (por ejemplo, un proyecto para un proceso empresarial fundamental, TIC, gestión de instalaciones u otros procesos de apoyo).

La gestión de proyectos utilizada debería requerir que:

a) los riesgos de seguridad de la información sean evaluados y tratados en una fase temprana y de forma periódica como parte de los riesgos del proyecto a lo largo de su ciclo de vida;

b) los requisitos de seguridad de la información [por ejemplo, los requisitos de seguridad de las aplicaciones (8.26), los requisitos de cumplimiento de los derechos de propiedad intelectual (5.32), etc.] sean atendidos en las primeras fases de los proyectos;

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

d) los avances en el tratamiento de los riesgos de seguridad de la información sean revisados y se evalúe y compruebe la eficacia del tratamiento.

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

Deberían definirse las responsabilidades y las autoridades en materia de seguridad de la información relevantes para el proyecto y asignarse a funciones específicas.

Se deberían identificar los requisitos de seguridad de la información para los productos o servicios entregados por el proyecto utilizando diversos métodos, incluyendo los derivados del cumplimiento de la política de seguridad de la información, las políticas específicas y la normativa. Otros requisitos de seguridad de la información pueden derivarse de actividades como el modelado de amenazas, la revisión de incidentes, el uso de umbrales de vulnerabilidad o planes de contingencia, garantizando así que la arquitectura y el diseño de los sistemas de información están protegidos contra las amenazas conocidas en función del entorno operativo.

Los requisitos de seguridad de la información deberían determinarse para todo tipo de proyectos, no sólo para los proyectos de desarrollo de TIC. A la hora de determinar estos requisitos, también habría que tener en consideración lo siguiente:

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

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

c) el nivel de confianza o garantía necesario en la identidad declarada de las entidades, a fin de obtener los requisitos de autenticación de usuarios;

d) los procesos de aprobación y autorización de acceso, tanto para clientes y otros usuarios potenciales del negocio como para los usuarios privilegiados o técnicos, como los miembros relevantes del proyecto, el personal potencial de operaciones o los proveedores externos;

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

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

g) los requisitos impuestos por otros controles de seguridad de la información (por ejemplo, interfaces para el registro y la monitorización o sistemas de detección de fugas de datos);

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

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

Información adicional

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

La Norma ISO/IEC 27005 ofrece orientación sobre el uso de los procesos de gestión de riesgos para identificar los controles que permitan cumplir los requisitos de seguridad de la información.

5.9 Inventario de información y otros activos asociados

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión_de_activos	#Gobernanza_y_Ecosistema #Protección

Control

Debería elaborarse y mantenerse un inventario de la información y otros activos asociados, incluyendo la identificación de sus propietarios.

Propósito

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

Orientación

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 ser mantenida en inventarios específicos o existentes según lo que sea adecuado.

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

a) La realización de revisiones periódicas de la información identificada y otros activos asociados con respecto al inventario de activos;

b) la aplicación automática de una actualización del inventario en el proceso de instalación, modificación o eliminación de un activo.

La ubicación de un activo debería ser incluida en el inventario según proceda.

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

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

La granularidad del inventario de la información y otros activos asociados alcanzar 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 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 ser asignada a un individuo o a un grupo y la clasificación deberías ser identificada (véanse 5.12, 5.13). Debería implementarse un proceso para garantizar la asignación oportuna de la propiedad de los activos. La propiedad debería asignarse cuando los activos son creados o cuando sean transferidos a la organización. La propiedad de los activos debería reasignarse según sea necesario cuando los propietarios actuales de los activos se marchen o cambien de puesto.

Obligaciones del propietario

El propietario debería ser responsable de la correcta gestión de un activo durante todo el ciclo de vida, garantizando que:

a) la información y otros activos asociados son inventariados;

b) la información y otros activos asociados se clasifican y protegen debidamente;

c) la clasificación es revisada periódicamente;

d) se enumeran y vinculan los componentes que soportan los activos tecnológicos, como la base de datos, el almacenamiento, los componentes y los subcomponentes de *software*;

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

f) las restricciones de acceso se corresponden con la clasificación y son efectivas y revisadas periódicamente;

g) cuando se elimine o deseche información y otros activos asociados, serán tratados de forma segura y suprimidos del inventario;

h) participan en la identificación y gestión de los riesgos asociados a su(s) activo(s);

i) apoyan al personal que tiene las funciones y responsabilidades de gestionar su información.

Información adicional

Los inventarios de información y otros activos asociados suelen ser necesarios para garantizar la efectiva protección de la información y pueden ser requeridos para otros propósitos, tales como por razones de salud, seguridad, seguros y financieras. También sirven de apoyo a la gestión de riesgos, las actividades de auditoría, la gestión de la vulnerabilidad, la respuesta a incidentes y la planificación de la recuperación.

Las tareas y responsabilidades pueden delegarse (por ejemplo, a un custodio al cuidado diario de los activos), pero la persona o el grupo que las ha delegado sigue siendo responsable.

Puede ser útil designar grupos de información y otros activos asociados que actúen conjuntamente para la prestación de un servicio concreto. En dicho caso, el propietario de dicho servicio es responsable de la prestación del servicio, incluyendo el funcionamiento de sus activos.

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

5.10 Uso aceptable de la información y activos asociados

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Gobernanza_y_Ecosistema #Protección

Control

Se deberían identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

Propósito

Garantizar que la información y otros activos asociados se protegen, utilizan y manejan adecuadamente.

Orientación

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

La organización debería establecer una política específica sobre el uso aceptable de la información y otros activos asociados y comunicarla a cualquier persona que utilice o maneje información y otros activos asociados. La política específica sobre el uso aceptable de la información debería proporcionar una dirección clara sobre cómo se espera que los individuos utilicen la información y otros activos asociados. La política específica debería indicar:

a) los comportamientos esperados e inaceptables de las personas desde el punto de vista de la seguridad de la información;

b) los usos permitidos y prohibidos de la información y otros activos asociados;

c) las actividades de monitorización realizadas por la organización.

Deberían redactarse procedimientos de uso aceptable para todo el ciclo de vida de la información en función de su clasificación (véase 5.12) y de los riesgos determinados. Los siguientes elementos deberían ser contemplados:

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

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

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

d) almacenamiento de los activos asociados a la información conforme a las especificaciones de sus fabricantes (véase 7.8);

e) clara identificación de todas las copias de los soportes de almacenamiento (electrónicos o físicos) para la atención del receptor autorizado (véase 7.10);

f) autorización para eliminar la información y otros activos asociados y método(s) de eliminación respaldados(s) (véase 8.10).

Información adicional

Puede darse el caso de que los activos en cuestión no pertenezcan directamente a la organización, como los servicios de la nube pública. El uso de dichos activos de terceros y cualquier activo de la organización asociado a dichos activos externos (por ejemplo, información, *software*) debería identificarse según corresponda y ser controlado, por ejemplo, mediante acuerdos con proveedores de servicios en la nube. También se debería tener cuidado cuando se utilice un entorno de trabajo colaborativo.

5.11 Devolución de activos

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

Control

Todos los empleados y otras terceras partes, según procedan, deberían devolver todos los activos de la organización en su poder tras el cambio o la terminación de su trabajo, contrato o acuerdo.

Propósito

Proteger los activos de la organización como parte del proceso de cambio o finalización del empleo, contrato o acuerdo.

Orientación

Debería estar formalizado un proceso de desvinculación que incluya la devolución de todos los activos físicos y electrónicos que sean propiedad de la organización o que estén bajo su custodia.

Cuando el personal y otras partes interesadas adquieran recursos de la organización o empleen sus propios recursos, deberían seguirse procedimientos para asegurar que toda la información relevante a rastreada, devuelta a la organización eliminada definitivamente de dichos recursos (véase 7.14).

Cuando el personal y otras partes interesadas tengan conocimiento sobre asuntos importantes para las operaciones en curso, deberían documentarse dichos conocimientos y ser transferidos a la organización.

La organización debería controlar la copia no autorizada de información relevante (por ejemplo, propiedad intelectual) durante el periodo entre la notificación de desvinculación del personal y la materialización efectiva de la misma.

La organización debería identificar y documentar claramente toda la información y otros activos asociados que deban devolverse, lo que puede incluir:

a) Dispositivos finales del usuario;

b) dispositivos de almacenamiento portátiles;

c) equipos especializados;

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

e) copias físicas de la información.

Información adicional

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

5.12 Clasificación de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Protección_de_la_información	#Protección #Defensa

Control

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

Propósito

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

Orientación

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

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

Las clasificaciones de la información y controles de protección asociados deberían tener en consideración las necesidades de negocio para compartir o restringir información, para proteger la integridad de la información y para garantizar la disponibilidad, así como los requisitos legales relativos a la confidencialidad, la integridad o la disponibilidad de la información. Los activos distintos a la información también pueden clasificarse de acuerdo con la clasificación de la información que almacena, procesa, manipula o protege.

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

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

El esquema debería estar alineado con la política específica de control de acceso (véase 5.1) y debería ser capaz de abordar las necesidades específicas de la organización.

La clasificación puede determinarse por el nivel de impacto que tendría para la organización la materialización de un riesgo sobre la información. Cada nivel definido en el esquema debería tener un título que tenga sentido en el contexto de la aplicación del esquema de clasificación.

El esquema debería ser homogéneo en toda la organización e incluido en sus procedimientos para que todo el mundo clasifique la información y demás activos asociados de la misma manera. De esta manera, todo el mundo tiene un entendimiento común de los requisitos de protección y aplica la protección apropiada.

El esquema de clasificación utilizado dentro de la organización puede ser diferente de los esquemas utilizados por otras organizaciones, incluso si la denominación de los niveles es similar. Además, la información que pasa de una organización a otra puede variar en cuanto a su clasificación dependiendo del contexto de cada organización, incluso si sus esquemas de clasificación son idénticos. Por lo tanto, los acuerdos con otras organizaciones que incluyan el intercambio de información deberían incluir procedimientos para identificar la clasificación de esa información e interpretar los niveles de clasificación de otras organizaciones. La correspondencia entre diferentes esquemas puede determinarse buscando la equivalencia en los métodos de tratamiento y protección asociados.

Información adicional

La clasificación proporciona a personas que tratan la información una indicación concisa sobre cómo debería tratarse y protegerse. La creación de grupos de información con necesidades de protección similares y la especificación de qué procedimientos de seguridad de la información se aplican a toda la información de cada grupo facilitan dicha clasificación. Esta aproximación reduce la necesidad de evaluaciones del riesgo caso por caso y el diseño de controles a medida.

La información puede dejar de ser sensible o crítica después de un determinado período de tiempo. Por ejemplo, cuando se ha difundido al público ya no tiene requisitos de confidencialidad, pero puede seguir requiriendo protección para sus propiedades de integridad y disponibilidad. Estos aspectos deberían ser tenidos en cuenta, ya que la clasificación excesiva puede conllevar a la implantación de controles innecesarios con un gasto adicional, o por el contrario una clasificación insuficiente puede llevar a que los controles sean insuficientes para proteger la información de cualquier peligro.

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

a) la revelación no conlleva daños;

b) la revelación causa un daño menor a la reputación o un impacto operacional menor;

c) la revelación tiene un impacto significativo a corto plazo sobre las operaciones u objetivos de negocio;

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

5.13 Etiquetado de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Protección_de_la_información	#Defensa #Protección

Control

Debería desarrollarse e implementarse un conjunto adecuado de procedimientos para el etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Propósito

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

Orientación

Los procedimientos de etiquetado de la información deberían contemplar la información y otros activos asociados en todos los formatos. El etiquetado debería corresponderse con el esquema de clasificación establecido en el apartado 5.12. Las etiquetas deberían ser fácilmente reconocibles. Los procedimientos deberían proporcionar directrices sobre cómo y dónde se vinculan las etiquetas, considerando cómo se accede a la información o cómo se tratan los activos dependiendo del tipo de soporte de almacenamiento. Los procedimientos pueden definir:

a) los casos en los que se omite el etiquetado (por ejemplo, el 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 en cualquier otro formato;

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

Algunos ejemplos de técnicas de etiquetado son:

a) etiquetas físicas;

b) encabezados y pies de página;

c) metadatos;

d) marcas de agua;

e) sellos.

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 la información. Los metadatos deberían facilitar que los sistemas interactúen y tomen decisiones basadas en las etiquetas de clasificación asociadas.

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

Los sistemas deberían añadir los metadatos adicionales pertinentes cuando procesen la información en función de 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 formación necesaria para garantizar que la información sea etiquetada correctamente y manipulada en consecuencia.

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

Información adicional

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

Otros metadatos útiles que pueden adjuntarse a la información son qué proceso organizativo creó la información y en qué momento.

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

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

5.14 Transferencia de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Protección

Control

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

Propósito

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

Orientación

General

La organización debería establecer y comunicar una política específica sobre la transferencia de información a todas las partes interesadas. Las normas, procedimientos y acuerdos para proteger la información en tránsito deberían reflejar la clasificación de la información en cuestión. Cuando la información se transfiera entre la organización y terceros, se deberían establecer y mantener acuerdos de transferencia (incluyendo la autenticación del destinatario) para proteger la información en todas sus formas en tránsito (véase 5.10).

La transferencia de información puede realizarse por medios electrónicos, físicos o verbales.

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

a) controles diseñados para proteger la información transferida de la interceptación, acceso no autorizado, copia, modificación, desvío, destrucción y denegación de servicio, incluyendo niveles de control de acceso acordes con la clasificación de la información que se trate y cualesquiera controles especiales que se requieran para proteger la información sensible, como el uso de técnicas criptográficas (véase 8.24);

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

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

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

e) el uso de un sistema de etiquetado acordado para la información sensible o crítica, que garantice que el significado de las etiquetas se entiende inmediatamente y que la información está debidamente protegida (véase 5.13);

f) un servicio de transferencia fiable y disponible;

g) una política específica sobre el uso aceptable de los servicios de transferencia de información (véase 5.10);

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

NOTA Puede existir legislación y normativa local en materia de conservación y eliminación de registros empresariales.

i) la consideración de cualquier otro requisito legal, estatutario, reglamentario y contractual pertinente (véanse 5.31, 5.32, 5.33, 5.34) relacionado con la transferencia de información (por ejemplo, requisitos de firma electrónica).

Transferencia electrónica

Las normas, procedimientos y acuerdos también deberían considerar los siguientes aspectos a la hora de utilizar los medios de comunicación electrónicos para la transferencia de información:

a) detección y protección contra código dañino que pueda transmitirse mediante el uso de comunicaciones electrónicas (véase 8.7);

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

c) prevención del envío de documentos y mensajes a una dirección o número erróneos;

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

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

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

g) aconsejar al personal y a otras partes interesadas de que no envíen SMS o mensajes instantáneos con información crítica, ya que puede ser leída en lugares públicos (y, por tanto, por personas no autorizadas) o almacenada en dispositivos no protegidos adecuadamente;

h) advertir al personal y a otras partes interesadas sobre los problemas que plantea la utilización de máquinas o servicios de fax, concretamente:

   1) el acceso no autorizado a los almacenes de mensajes integrados para la recuperación de mensajes;

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

Transferencia de soportes físicos de almacenamiento

Cuando se transfieran soportes físicos de almacenamiento (incluido el papel), las normas, procedimientos y acuerdos deberían incluir:

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

b) garantizar el correcto direccionamiento y transporte del mensaje;

c) embalajes que protejan el contenido de cualquier daño físico que pueda producirse durante el transporte y de conformidad con las especificaciones de los fabricantes, por ejemplo, protegiéndolo de cualquier factor ambiental que pueda reducir la eficacia de los medios de almacenamiento de restauración, como la exposición al calor, la humedad o los campos electromagnéticos; utilizando normas técnicas mínimas para el embalaje y la transmisión (por ejemplo, el uso de sobres opacos);

d) una lista de mensajeros fiables autorizados aprobada por la dirección;

e) normas de identificación del mensajero;

f) en función del nivel de clasificación de la información contenida en los soportes de almacenamiento que vaya a transportarse, utilizar controles a prueba de manipulaciones (por ejemplo, bolsas, contenedores);

g) procedimientos para verificar la identificación de los mensajeros;

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

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

Transferencia verbal

Para proteger la transferencia verbal de información, debería recordarse al personal y a otras partes interesadas que deberían:

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

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

c) reproducir a un nivel adecuado que permita escuchar la conversación;

d) asegurar la aplicación de los controles adecuados en la sala (por ejemplo, insonorización, puerta cerrada);

e) iniciar las conversaciones confidenciales con un descargo de responsabilidad para que los presentes conozcan el nivel de clasificación y los requisitos de tratamiento de lo que van a escuchar.

Información adicional

Ninguna información adicional.

5.15 Control de acceso

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_gestión_de_acceso	#Protección

Control

Se deberían establecer e implementar reglas de control de acceso físico y lógico a la información y a otros activos asociados, basadas en los requisitos de negocio y de seguridad de la información.

Propósito

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

Orientación

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

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

a) determinar qué tipo de acceso a la información y a otros activos asociados requiere cada entidad;

b) la seguridad de las aplicaciones (véase 8.26);

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

d) la diseminación y autorización de la información (por ejemplo, el principio “algo que sabes”) y los niveles de seguridad y de clasificación de la información (véanse 5.10, 5.12 y 5.13);

e) las restricciones al acceso privilegiado (véase 8.2);

f) la segregación de funciones (véase 5.3);

g) la legislación y normativas aplicables y cualquier obligación contractual relativa a la limitación de acceso a datos o servicios (véanse 5.31, 5.32, 5.33, 5.34 y 8.3);

h) la segregación de funciones en el control de acceso (por ejemplo, la petición de acceso, la autorización de acceso, la administración de acceso);

i) la autorización formal de las peticiones de acceso (véanse 5.16 y 5.18);

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

k) el registro (véase 8.15).

Las reglas de control de acceso deberían implementarse definiendo y asignando los derechos y restricciones de acceso adecuados a las entidades pertinentes (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 funciones específicas a grupos de entidades.

A la hora de definir y aplicar las reglas de control de acceso se debería tener en consideración lo siguiente:

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

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

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

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

Información adicional

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

a) “algo que sabes”: sólo se da acceso a aquella información necesaria para la entidad para realizar las tareas (diferentes tareas o roles recogen diferentes ‘necesidades de conocer’ y por tanto diferentes perfiles de acceso);

b) “algo que necesitas”: sólo se asigna a una entidad el acceso a la infraestructura de tecnología de la información en los casos en que existe una necesidad clara.

Se debería tener cuidado al especificar las reglas de control de acceso, considerando:

a) el establecimiento de reglas basadas en la premisa del menor privilegio, “Todo está prohibido a no ser que se permita expresamente” en vez de la regla más débil “Todo está permitido a no ser que se prohíba expresamente”;

b) los cambios en el etiquetado de la información (véase 5.13) realizados automáticamente por las instalaciones de tratamiento de la información y los iniciados a discreción del usuario;

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

d) cuando definir y revisar periódicamente la aprobación.

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

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

Las reglas de control de acceso también pueden contener elementos dinámicos (por ejemplo, una función que evalúa los accesos anteriores o valores específicos del entorno). Las reglas de control de acceso se pueden implementar con distinta granularidad, desde la cobertura total de redes o sistemas hasta campos de datos específicos, y también pueden tener en consideración propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso. Estos principios y la forma en que se define el control de acceso granular pueden tener un impacto significativo en los costes. Unas reglas más estrictas y una mayor granularidad suelen suponer un mayor coste. Los requisitos de negocio y las consideraciones de riesgo se deberían utilizar para definir qué reglas de control de acceso se aplican y qué granularidad se requiere.

5.16 Gestión de identidad

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_gestión_de_acceso	#Protección

Control

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

Propósito

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

Orientación

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

a) en el caso de las identidades asignadas a personas, una identidad específica sólo esté vinculada a una única persona para poder responsabilizarla de las acciones realizadas con esa identidad específica;

b) las identidades asignadas a múltiples personas (por ejemplo, las identidades compartidas) sólo estén permitidas cuando son necesarias por razones empresariales u operativas y estén sujetas a una aprobación y documentación específicas;

c) las identidades asignadas a entidades no humanas estén sujetas a una aprobación debidamente segregada y a una supervisión permanente independiente;

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

e) en un ámbito específico, se asigne una única identidad a una única entidad, [es decir, evitar la asignación de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)];

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

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

Cuando se utilicen identidades proporcionadas o emitidas por terceros (por ejemplo, credenciales de redes sociales), la organización debería garantizar que las identidades de terceros proporcionan el nivel de confianza requerido y que cualquier riesgo asociado es conocido y abordado. Esto puede incluir controles relacionados con los terceros (véase 5.19), así como controles relacionados con la información de autenticación asociada (véase 5.17).

Información adicional

Proporcionar o revocar el acceso a la información y a otros activos asociados consta habitualmente de varias fases:

a) confirmar los requisitos de negocio para establecer una identidad;

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

c) establecer una identidad;

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

e) proveer o revocar los derechos de acceso específicos a la identidad, basándose en las decisiones de autorización o habilitación adecuadas (véase 5.18).

5.17 Información de autenticación

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_gestión_de_acceso	#Protección

Control

La asignación y gestión de la información de autenticación debería controlarse mediante un proceso formal de gestión, incluyendo el asesoramiento al personal sobre el tratamiento adecuado de la información de autenticación.

Propósito

Garantizar la correcta autenticación de las entidades y evitar fallos en los procesos de autenticación.

Orientación

Asignación de la información de autenticación

El proceso de asignación y gestión debería garantizar que:

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

b) se establezcan procedimientos para verificar la identidad de un usuario antes de proporcionarle información de autenticación nueva, de sustitución o provisional;

c) la información de autenticación, incluida la información de autenticación temporal, sea transmitida a los usuarios de forma segura (por ejemplo, a través de un canal autenticado y protegido) evitando el uso de correos electrónicos no protegidos (texto sin cifrar);

d) los usuarios confirmen la recepción de la información de autenticación;

e) la información de autenticación por defecto, predefinida o proporcionada por los proveedores, se cambie inmediatamente después de la instalación de los sistemas o del *software*;

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

Responsabilidades del usuario

Toda persona que tenga acceso a la información de autenticación o que la utilice debería asegurarse de que:

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

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

c) cuando se usen contraseñas como información de autenticación, crear contraseñas fuertes de acuerdo con las recomendaciones de las mejores prácticas, por ejemplo:

    1) que las contraseñas no estén basadas en algo que alguien más pueda adivinar con facilidad u obtener usando información asociada a la persona (por ejemplo, nombres, números de teléfono, fechas de nacimiento);

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

    3) utilizar frases de contraseña fáciles de recordar y tratar de incluir caracteres alfanuméricos y especiales;

    4) que las contraseñas tengan una longitud mínima;

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

e) que la obligación de seguir estas normas se incluya también en las condiciones de empleo (véase 6.2).

Sistema de gestión de contraseñas

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

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

b) imponer contraseñas seguras según las recomendaciones de buenas prácticas [véase c) de "Responsabilidades del usuario"];

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

d) obligar a cambiar las contraseñas cuando sea necesario, por ejemplo, después de un incidente de seguridad, o en caso de cese o cambio de empleo cuando un usuario tenga contraseñas conocidas para identidades que permanezcan activas (por ejemplo, identidades compartidas);

e) evitar la reutilización de contraseñas anteriores;

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

g) no mostrar las contraseñas en la pantalla cuando se están introduciendo;

h) almacenar y transmitir las contraseñas en forma protegida.

El cifrado y el hashing de las contraseñas deberían realizarse de acuerdo con las técnicas criptográficas aprobadas para las contraseñas (véase 8.24).

Información adicional

Las contraseñas o frases de contraseña son un tipo de información de autenticación comúnmente utilizado y habitual para verificar la identidad de un usuario. Otros medios de autenticación son las claves criptográficas, los datos almacenados en dispositivos (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación y los datos biométricos como los escaneos del iris o las huellas dactilares. Se puede encontrar información adicional en la Norma ISO/IEC 24760.

Exigir el cambio frecuente de las contraseñas puede ser problemático porque los usuarios pueden molestarse por los cambios frecuentes, olvidar las nuevas contraseñas, anotarlas en lugares poco seguros o elegir contraseñas poco seguras. La implementación de un inicio de sesión único (SSO) u otras herramientas de gestión de la autenticación (por ejemplo, almacén de contraseñas) reduce la cantidad de información de autenticación que los usuarios tienen que proteger, incrementando por consiguiente la efectividad de este control. Sin embargo, estas herramientas pueden incrementar también el impacto de divulgar la información de autenticación.

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

5.18 Derechos de acceso

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_gestión_de_acceso	#Protección

Control

Los derechos de acceso a la información y otros activos asociados deberían aprovisionarse, revisarse, modificarse y eliminarse de conformidad con la política específica de la organización y las reglas sobre control de acceso.

Propósito

Garantizar que el acceso a la información y a otros activos asociados es definido y autorizado de acuerdo con los requisitos del negocio.

Orientación

Provisión y revocación de los derechos de acceso

El proceso para la asignación o revocación de derechos de acceso físicos y lógicos concedidos a la identidad autenticada de una entidad debería:

a) obtener la autorización del propietario de la información y otros activos asociados para el uso de ésta (véase 5.9). Puede ser apropiada la aprobación adicional y por separado por parte de la dirección, de los derechos de acceso;

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

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

d) garantizar que los derechos de acceso son eliminados cuando alguien no necesita acceder a la información y a otros activos asociados, en particular garantizando que los derechos de acceso de los usuarios que han dejado la organización son eliminados en el momento oportuno;

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

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

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

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

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

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

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

Revisión de los derechos de acceso

Las revisiones periódicas de los derechos de acceso físicos y lógicos deberían tener en consideración lo siguiente:

a) los derechos de acceso de los usuarios después de cualquier cambio dentro de la organización (por ejemplo, cambio de trabajo, promoción, degradación) o finalización del empleo (véanse los puntos 6.1 a 6.5);

b) las autorizaciones de derechos de acceso privilegiados.

Observaciones antes de cambiar o terminar la relación laboral

Los derechos de acceso de un usuario a la información y a otros activos asociados deberían ser revisados y ajustados o eliminados antes de cambiar o terminar la relación laboral, basándose en la evaluación de factores de riesgo tales como:

a) si la finalización o el cambio de puesto de trabajo la inicia el usuario o la dirección así como la razón para la finalización;

b) las responsabilidades actuales del usuario;

c) el valor de los activos accesibles en ese momento.

Información adicional

Se debería considerar el establecimiento de roles de acceso de usuarios basados en los requisitos del negocio, de forma que agrupen varios derechos de acceso en perfiles de acceso de usuarios típicos. Las peticiones y revisiones de los derechos de acceso son más fáciles de gestionar a nivel de roles que a nivel de derechos particulares.

Se debería considerar la inclusión de cláusulas en los contratos de personal y en los contratos de servicios que especifiquen las sanciones en caso de que el personal intente realizar un acceso no autorizado (véase 5.20, 6.2, 6.4, 6.6).

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

La clonación es una forma eficaz de que las organizaciones asignen acceso a los usuarios. Sin embargo, debería hacerse con cuidado, basándose en los distintos roles identificados por la organización, en lugar de limitarse a clonar una identidad con todos los derechos de acceso asociados. La clonación tiene el riesgo inherente de dar lugar a un exceso de derechos de acceso a la información y otros activos asociados.

5.19 Seguridad de la información en las relaciones con los proveedores

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_la_relación_con_los_proveedores	#Gobernanza_y_Ecosistema #Protección

Control

Se deberían identificar e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios de proveedores.

Propósito

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

Orientación

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

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 de recursos de proveedores de servicios en la nube por parte de la organización. Estos procesos y procedimientos deberían ser implementados por la organización y requeridos a los proveedores de servicios, tanto al inicio como a la finalización del uso de sus productos o servicios. Como por ejemplo:

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

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

c) evaluar y seleccionar aquellos productos o servicios de los proveedores que tengan controles de seguridad de la información adecuados y revisarlos; en particular, la exactitud y la exhaustividad de los controles aplicados por el proveedor que garanticen la integridad de la información y de su tratamiento y, por tanto, la seguridad de la información de la organización;

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

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

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

    1) el uso por parte de los proveedores de la información de la organización y otros activos asociados, incluyendo los riesgos originados por el eventual mal uso intencionado del personal del proveedor;

    2) el mal funcionamiento o las vulnerabilidades de los productos (incluyendo los componentes y subcomponentes de *software* utilizados en estos productos) o los servicios prestados por los proveedores;

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

h) mitigar el incumplimiento de un proveedor, ya sea detectado a través de la monitorización o por otros medios;

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

j) los acuerdos de resiliencia y, si fuesen necesarias, las medidas de recuperación y de contingencia para garantizar la disponibilidad de la información y el procesamiento de la información del proveedor y, por tanto, la disponibilidad de la información de la organización;

k) las sesiones de concienciación para el personal de la organización que interactúa con el personal de los proveedores con respecto a las reglas apropiadas referentes al acuerdo las políticas, procesos y procedimientos específicos según el tipo de proveedor y el nivel de acceso de estos a los sistemas y a la información de la organización;

l) la gestión de las transferencias de información necesarias, de otros activos asociados y de cualquier otro elemento que deba ser modificado, y garantizar que la seguridad de la información se mantenga durante todo el período de transferencia;

m) los requisitos para garantizar un cese seguro de la relación con el proveedor, incluyendo:

   1) la retirada de los derechos de acceso;

   2) el tratamiento de la información;

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

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

   5) la gestión de registros;

   6) la devolución de activos;

   7) la eliminación segura de la información y otros activos asociados;

   8) los requisitos de confidencialidad en curso;

n) el nivel de seguridad del personal y la seguridad física que se espera del personal del proveedor y de sus instalaciones.

Deberían considerarse procedimientos para continuar con el tratamiento 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 a causa de los avances tecnológicos), para evitar cualquier retraso en la organización de productos o servicios de sustitución (por ejemplo, identificando un proveedor alternativo por adelantado o utilizando siempre proveedores alternativos).

Información adicional

En los casos en que sea imposible que una organización imponga requisitos a un proveedor, la organización debería:

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

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

Los proveedores pueden poner en riesgo la información con una gestión inadecuada de la seguridad de la información. Deberían identificarse y aplicarse controles para administrar el acceso de proveedores a la información y a otros activos asociados. Por ejemplo, si hay una necesidad especial de garantizar la confidencialidad de la información, se pueden utilizar acuerdos de confidencialidad o técnicas criptográficas. Otro ejemplo es el riesgo en materia de protección de datos cuando el acuerdo con el proveedor implique la transferencia o el acceso a la información a nivel internacional. La organización tiene que ser consciente de que la responsabilidad legal o contractual de proteger la información permanece en la organización.

Los riesgos también pueden ser causados por controles inadecuados de los componentes de la infraestructura de las TIC o de los servicios prestados por los proveedores. El mal funcionamiento o la vulnerabilidad de los componentes o servicios pueden provocar violaciones de la seguridad de la información en la organización o en otra entidad (por ejemplo, pueden causar una infección de código dañino, ataques u otros daños en entidades distintas de la organización).

Véase la Norma ISO/IEC 27036-2 para más detalles.

5.20 Abordar la seguridad de la información dentro de los acuerdos de proveedores

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_la_relación_con_los_proveedores	#Gobernanza_y_Ecosistema #Protección

Control

Deberían establecerse y acordarse con cada proveedor los requisitos pertinentes de seguridad de la información 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.

Orientación

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

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

a) Descripción de la información facilitada o accedida y los métodos para facilitar o acceder a la información;

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

c) relación entre el propio esquema de clasificación de la organización con el esquema de clasificación del proveedor;

d) los requisitos legales, estatutarios, regulatorios, así como los contractuales, incluyendo la protección de datos personales, el tratamiento de la información personal identificable (PII), los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se garantizará que se cumplen;

e) la obligación contractual de cada parte para implementar un conjunto acordado de controles incluyendo el control de acceso, la evaluación del desempeño, la supervisión, los informes y la auditoria y las obligaciones del proveedor de cumplir los requisitos de seguridad de la información de la organización;

f) normas sobre el uso aceptable de la información y otros activos asociados, incluyendo el uso inaceptable si fuese necesario;

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

h) requisitos de seguridad de la información relativos 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 que sirvan de base para los acuerdos individuales con el proveedor, basados en las necesidades de negocio y los criterios de riesgo de la organización;

i) indemnizaciones y subsanaciones en caso de que el contratista incumpla los requisitos;

j) requisitos y procedimientos de gestión de incidentes (en especial de notificación y colaboración durante la subsanación de los incidentes);

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

l) disposiciones relevantes para la subcontratación, incluidos los controles que necesiten ser implementados, como el acuerdo sobre el uso de subcontratistas (por ejemplo, exigiendo que estén bajo las mismas obligaciones del proveedor, exigiendo tener una lista de subcontratistas y de notificación ante cualquier cambio);

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

n) cualquier requisito de investigación del personal, cuando esté legalmente permitido, para el personal del proveedor, incluyendo responsabilidades para llevar a cabo la investigación y los procedimientos de notificación si la investigación no se ha completado o si los resultados dan lugar a dudas o preocupaciones;

o) las evidencias y mecanismos de garantía de las certificaciones de terceros para los requisitos de seguridad de la información pertinentes relacionados con los procesos del proveedor y un informe independiente sobre la eficacia de los controles;

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

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

r) procesos de resolución de contrato por defecto y por conflictos;

s) proporcionar una copia de seguridad en consonancia con las necesidades de la organización (en términos de frecuencia, tipo y ubicación de almacenamiento);

t) garantizar la disponibilidad de una instalación alternativa (es decir, un centro de recuperación en caso de catástrofe) que no esté sometida a las mismas amenazas que la instalación principal y que tenga en cuenta los controles secundarios (controles alternativos) en caso de que fallen los controles primarios;

u) disponer de un proceso de gestión de cambios que garantice la notificación previa a la organización y la posibilidad de que ésta no acepte los 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 la transmisión lógica;

x) cláusulas de rescisión tras la conclusión del acuerdo, incluyendo la gestión de los registros, la devolución de los activos, la eliminación segura de la información y otros activos asociados, y cualquier obligación relativa a la confidencialidad;

y) provisión de un método de destrucción seguro de la información de la organización almacenada por el proveedor tan pronto como deje de ser necesaria;

z) garantizar, al final del contrato, la transferencia del soporte a otro proveedor o a la propia organización.

La organización debería establecer y mantener un registro de acuerdos con partes externas (por ejemplo, contratos, memorándum de entendimiento, acuerdos de intercambio de información) para hacer un seguimiento del destino de su información. La organización también debería revisar, validar y actualizar periódicamente sus acuerdos con partes externas para asegurarse de que siguen siendo necesarios y de que se ajustan a su finalidad con las cláusulas de seguridad de la información pertinentes.

Información adicional

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

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

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_ la_ relación_con_los_proveedores	#Gobernanza_y_Ecosistema #Protección

Control

Se deberían definir e implementar procesos y procedimientos para hacer frente a los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de Tecnologías de la Información y de las Comunicaciones (TIC).

Propósito

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

Orientación

Para abordar la seguridad de la información en el marco de la seguridad de la cadena de suministro de las TIC, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores, deberían considerarse los siguientes temas:

a) la definición de requisitos de seguridad de la información para aplicar durante 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 prestado a la organización;

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

d) solicitar a los proveedores de productos de TIC que proporcionen información acerca de los componentes de *software* utilizados en sus productos;

e) solicitar a los proveedores de productos de TIC que proporcionen información que describa las funciones de seguridad implementadas en su producto y la configuración necesaria para su funcionamiento seguro;

f) implementar un proceso de supervisión y métodos aceptables para validar que los productos y servicios de TIC suministrados cumplan los requisitos de seguridad establecidos. Algunos ejemplos de estos métodos de revisión de los proveedores pueden ser las pruebas de penetración y la prueba o validación de los certificados de terceros para las operaciones de seguridad de la información del proveedor;

g) la implementación de un proceso de identificación de componentes críticos de productos o servicios para el mantenimiento de la funcionalidad y que, por tanto, requieren una mayor atención, escrutinio y seguimiento adicional cuando se construyen fuera de la organización, especialmente si el proveedor subcontrata partes del producto o componentes del servicio a otros proveedores;

h) obtener garantías de que los componentes críticos y su origen son rastreables a lo largo de la cadena de suministro;

i) obtener garantías de que los productos de TIC suministrados funcionan como se espera sin ningún tipo de características inesperadas o no deseadas;

j) implementar procesos que garanticen que los componentes de los proveedores son auténticos y no han sido alterados con respecto a su especificación. Algunos ejemplos de medidas son las etiquetas anti-falsificación, las verificaciones de hash criptográfico o las firmas digitales. El control de las prestaciones fuera de especificación puede ser un indicador de manipulación o falsificación. La prevención y la detección de manipulaciones debería aplicarse en múltiples etapas del ciclo de vida de desarrollo del sistema, incluyendo el diseño, desarrollo, integración, operaciones y mantenimiento;

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

l) definir reglas para el intercambio de información con respecto a la cadena de suministro y la gestión de posibles problemas y compromisos entre la organización y los proveedores;

m) la implantación de procesos específicos para la gestión de la información y el ciclo de vida, la disponibilidad y los riesgos de seguridad asociados a los componentes de TIC. Esto incluye la gestión de los riesgos de aquellos componentes que dejen de estar disponibles, debido al cese de negocio de los proveedores, o a que los proveedores no entreguen ya estos componentes por obsolescencia tecnológica. Debería considerarse la identificación de un proveedor alternativo y el proceso para transferir el *software* y la competencia al proveedor alternativo.

Información adicional

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

Se recomienda a las organizaciones trabajar con los proveedores para entender la cadena de suministro de TIC y todas las cuestiones que tienen un efecto importante sobre los productos y servicios que se proporcionen. 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 ser abordado por otros proveedores en la cadena de suministro TIC.

Las TIC deberían ser adquiridas de fuentes acreditadas. La fiabilidad del *software* y el *hardware* es una cuestión de control de calidad. Aunque generalmente no es posible que una organización inspeccione los sistemas de control de calidad de sus proveedores, puede hacer juicios fiables basados en la reputación del proveedor.

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

Algunos ejemplos de cadenas de suministro de TIC son:

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

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

c) servicios de alojamiento, en los que el proveedor se apoya en servicios de asistencia externos que incluyen el primer, segundo y tercer nivel de apoyo.

Consulte la Norma ISO/IEC 27036-3 para obtener más detalles, incluida la orientación para la 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, proporcionando información sobre la procedencia del *software*. Véase la Norma ISO/IEC 19770-2 para más detalles.

5.22 Seguimiento, revisión y gestión del cambio de los servicios de proveedores

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_la_relación_con_los_proveedores #Garantía_de_seguridad_de_la_información	#Gobernanza_y_Ecosistema#Protección #Defensa

Control

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

Propósito

Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

Orientación

La supervisión, revisión y gestión de cambios de los servicios de los proveedores deberían asegurar el cumplimiento de las condiciones de seguridad de la información de los acuerdos, la gestión adecuada de los incidentes y problemas de seguridad de la información y que los cambios en los servicios de los proveedores o en la situación de la empresa no afecten a la prestación del servicio.

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

a) supervisar los niveles de rendimiento del servicio para verificar el cumplimiento de los acuerdos;

b) supervisar los cambios realizados por los proveedores, incluyendo:

   1) las mejoras de los servicios ofrecidos actualmente;

   2) el desarrollo de nuevas aplicaciones y sistemas;

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

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

c) supervisar los cambios en los servicios de los proveedores, incluyendo:

   1) los cambios y mejoras en las redes;

   2) el uso de nuevas tecnologías;

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

   4) nuevas herramientas y entornos de desarrollo;

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

   6) cambio de proveedores;

   7) subcontratación de otro proveedor;

d) revisar los informes del servicio producidos por el proveedor y organizar reuniones periódicas de progreso según sea requerido en los acuerdos;

e) llevar a cabo auditorías de los proveedores y proveedores subcontratados, junto con la revisión de los informes de auditoría independiente, si están disponibles, y el seguimiento de las cuestiones identificadas;

f) proporcionar información sobre los incidentes de seguridad de la información y revisar esta información según sea requerido en los acuerdos y las directrices y procedimientos de soporte;

g) revisar las pistas de auditoría de los proveedores y los registros de eventos de seguridad de la información, problemas operativos, fallos, registros de los errores e interrupciones relacionadas con el servicio prestado;

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

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

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

k) asegurar que el proveedor mantenga la capacidad de servicio suficiente, junto con planes viables destinados a garantizar que los niveles de continuidad de servicio acordados se mantengan después de fallos mayores de los servicios o de desastre (véanse 5.29, 5.30, 5.35, 5.36 y 8.14);

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

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

La responsabilidad de la gestión de las relaciones con los proveedores se debería asignar a una persona individual o equipo específico. Deberían estar disponibles los suficientes recursos técnicos para supervisar, en particular, que se están cumpliendo los requisitos de seguridad de la información del acuerdo. Se deberían tomar las medidas apropiadas cuando se observan deficiencias en la prestación de servicios.

Información adicional

Véase la Norma ISO/IEC 27036-3 para más detalles.

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

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_ la_ relación_con_los_proveedores	#Gobernanza_y_Ecosistema #Protección

Control

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

Propósito

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

Orientación

La organización debería establecer y comunicar la política específica en el uso de los servicios en la nube a todas partes interesadas.

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

El uso de servicios en la nube puede implicar compartir la responsabilidad de la seguridad de la información y las actividades 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 de ambos, el proveedor del servicio en la nube y la organización, que actúa como cliente del servicio en la nube, estén definidas e implementadas de forma adecuada.

La organización debería definir:

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

b) los criterios para la selección del servicio en la nube y el alcance del uso del servicio en la nube;

c) los roles y responsabilidades relacionados con el uso y la gestión de los servicios en la nube;

d) los controles de seguridad de la información que son gestionados por el proveedor del servicio en la nube y los que son gestionados por la organización como cliente del servicio en la nube;

e) cómo obtener y utilizar las capacidades de seguridad de la información prestadas por el proveedor del servicio en la nube;

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

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

h) los procedimientos para la gestión de incidentes de seguridad de la información que ocurran en relación al uso de servicios en la nube;

i) el enfoque para la monitorización, la revisión y la evaluación del uso continuado de los servicios en la nube en la gestión de riesgos de seguridad de la información;

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

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

Un acuerdo entre el proveedor del servicio 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) suministro de soluciones para la arquitectura e infraestructura basadas en normas aceptadas por la industria;

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

c) ejecución de soluciones de protección y monitorización de código malicioso;

d) procesamiento y almacenamiento de la información sensible de la organización en ubicaciones autorizadas (por ejemplo, una región o país concreto) o sujetas a una jurisdicción concreta;

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

f) garantía del cumplimiento de los requisitos de seguridad de la información de la organización en el caso de que los servicios en la nube sean subcontratados a un proveedor externo (o prohibición de la subcontratación de los servicios en la nube);

g) apoyo a la organización en la recogida de la evidencia digital, teniendo en cuenta las leyes y los reglamentos para la recogida de la evidencia digital de las diferentes jurisdicciones;

h) prestación adecuada del soporte y la disponibilidad de los servicios durante un período de tiempo oportuno cuando la organización quiere salir de los servicios en la nube;

i) suministro de copia de seguridad de los datos y de la información de configuración requeridos y gestión de forma segura de las copias de seguridad, según corresponda, y en función de las capacidades del proveedor del servicio en la nube utilizado por la organización, que actúa como cliente del servicio en la nube;

j) provisión y devolución de información como ficheros de configuración, código fuente y datos que son propiedad de la organización, que actúa como cliente del servicio en la nube, cuando son solicitados durante la prestación o finalización del servicio.

La organización, que actúa como cliente del servicio en la nube, debería considerar si el acuerdo debiese 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, incluyendo:

a) los cambios en la infraestructura técnica (por ejemplo, reubicación, reconfiguración, o cambios en el *hardware* o *software*) que afectan o modifican la oferta del servicio en la nube;

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

c) el uso de proveedores de servicios en la nube similares u otros subcontratados (incluido el cambio de los existentes o el uso de nuevos).

La organización que utiliza servicios en la nube debería mantener un contacto estrecho 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, incluyendo un mecanismo tanto para el proveedor del servicio en la nube como para la organización, que actúa como cliente del servicio en la nube, para monitorizar cada característica del servicio e informar de defectos en el cumplimiento de los compromisos contenidos en los acuerdos.

Información adicional

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

Es posible encontrar información adicional relacionada con servicios en la nube en las Normas ISO/IEC 17788, ISO/IEC 17789 y ISO/IEC 22123-1. Aspectos específicos relacionados con la portabilidad del servicio en la nube durante las estrategias de salida se encuentran en la Norma ISO/IEC 19941. Aspectos específicos relacionados con seguridad de la información y servicios públicos en la nube se describen en la Norma ISO/IEC 27017. Aspectos específicos relacionados con la protección de la PII en la nube pública actuando como Encargado del Tratamiento se describe en la Norma ISO/IEC 27018. Las relaciones con el proveedor de servicios en la nube se incluyen en ISO/IEC 27036-4 y los acuerdos de servicios en la nube y sus contenidos se abordan en la serie de Normas ISO/IEC 19086, abordando específicamente la seguridad y la privacidad en la Norma ISO/IEC 19086-4.

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

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Governanza #Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

La organización debería planificar y prepararse para gestionar los incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de los procesos, roles y responsabilidades de gestión de los incidentes de seguridad de la información.

Propósito

Asegurar la respuesta rápida, efectiva, consistente y adecuada a los incidentes de seguridad de la información, incluyendo la comunicación de los eventos de seguridad de la información.

Orientación

Roles y responsabilidades

La organización debería establecer procesos adecuados para la gestión de incidentes de seguridad de la información. Los roles y las responsabilidades para llevar a cabo los procedimientos de gestión de incidentes deberían definirse y comunicarse de forma efectiva a las partes relevantes interesadas internas y externas.

Debería considerarse lo siguiente:

a) establecer un método común para la notificación de eventos de seguridad de la información incluyendo el punto de contacto (véase 6.8);

b) establecer un proceso de gestión de incidentes para proporcionar a la organización con capacidad para gestionar los incidentes de seguridad incluyendo la administración, la documentación, la detección, el triaje, la priorización, el análisis, la comunicación y la coordinación con las partes interesadas;

c) establecer un proceso de respuesta a incidentes para proporcionar a la organización con capacidad para la evaluación, la respuesta y el aprendizaje de los incidentes de seguridad de la información;

d) permitir solo al personal competente el manejo de los asuntos relacionados con los incidentes de seguridad de la información de la organización. Este personal debería recibir la documentación de los procedimientos y capacitación periódica;

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

Procedimientos de gestión de incidentes

Los objetivos de la gestión de incidentes de seguridad de la información deberían ser acordados con la dirección, y debería garantizarse que los responsables de la gestión de incidentes de seguridad de la información comprenden las prioridades de la organización en cuanto al tratamiento de los incidentes de seguridad de la información, incluyendo el periodo de tiempo de la resolución en función de las potenciales consecuencias y severidad del incidente. Los procedimientos de gestión de incidentes deberían implementarse para cumplir con estos objetivos y prioridades.

La dirección debería asegurar que el plan para la gestión de incidentes de seguridad de la información se crea considerando diferentes escenarios y los procedimientos son desarrollados e implementados por las siguientes actividades:

a) evaluación de los eventos de seguridad de la información de acuerdo a los criterios de aquello que constituye un incidente de seguridad de la información;

b) monitorización (véase 8.15 y 8.16), detección (véase 8.16), clasificación (véase 5.25), análisis y notificación (véase 6.8) de los eventos de seguridad de la información (por medios humanos o automáticos);

c) gestión de los incidentes de seguridad de la información hasta su cierre, incluidos la respuesta y el escalado (véase 5.26) de acuerdo al tipo y categoría del incidente, la posible activación de la gestión de crisis y de los planes de continuidad de negocio, la recuperación controlada a partir de un incidente y la comunicación a las partes interesadas internas y externas;

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

e) registro de las actividades de la gestión del incidente;

f) manejo de evidencias (véase 5.28);

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

h) identificación de lecciones aprendidas y cualquier mejora para el procedimiento de gestión de incidentes o para los controles de seguridad de la información en general que sean necesarias.

Procedimientos de notificación

Los procedimientos de notificación deberían incluir:

a) las acciones que realizar en caso de un evento de seguridad de la información (por ejemplo, anotar todos los detalles pertinentes como errores de funcionamiento y mensajes en la pantalla, notificar inmediatamente al punto de contacto y solo adoptar acciones coordinadas);

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

c) los procesos de retroalimentación apropiados para garantizar que las personas que informan sobre eventos de seguridad de la información sean notificadas, en la medida de lo posible, de los resultados después de que se haya abordado y cerrado el problema;

d) la creación de informes de incidentes.

En la implementación de los procedimientos de la gestión de incidentes debería considerarse cualquier requisito externo en la notificación de incidentes a las partes relevantes interesadas dentro del periodo de tiempo definido (por ejemplo, requisitos de notificación de un incumplimiento a los reguladores).

Información adicional

Los incidentes de seguridad de la información pueden transcender los límites de la organización o del país. Para reaccionar ante dichos incidentes, es beneficioso coordinar la respuesta y compartir la información acerca de estos incidentes con organizaciones externas, cuando esto sea apropiado.

Una guía detallada sobre la gestión de incidentes de seguridad de la información está disponible en la Norma ISO/IEC 27035.

5.25 Evaluación y decisión sobre los eventos de seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

La organización debería evaluar los eventos de seguridad de la información y decidir si deben ser catalogados como incidentes de seguridad de la información.

Propósito

Asegurar la categorización y la priorización efectiva de los eventos de seguridad de la información.

Orientación

El esquema de categorización y priorización de los eventos de seguridad de la información debería acordarse para la identificación de las consecuencias y la prioridad de un incidente. El esquema debería incluir los criterios para categorizar los 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 la coordinación y la respuesta de 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 decisión deberían registrarse con todo detalle a efectos de futuras referencias y verificación.

Información adicional

La serie de Normas ISO/IEC 27035 proporciona una guía adicional sobre la gestión de incidentes.

5.26 Respuesta a incidentes de seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.

Propósito

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

Orientación

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

Los incidentes de seguridad de la información deberían responderse por el equipo designado y con las competencias necesarias (véase 5.24).

La respuesta debería incluir lo siguiente:

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

b) recogida de evidencias (véase 5.28) tan pronto como sea posible tras la ocurrencia del incidente;

c) escalado del incidente, si así se requiere, incluyendo las actividades de la gestión de crisis y posiblemente invocando planes de continuidad del negocio (véase 5.29 y 5.30);

d) aseguramiento de que todas las actividades de respuesta se registran adecuadamente para realizar el correspondiente análisis posterior;

e) comunicación de la existencia del incidente de seguridad de la información o cualquier otro detalle relevante del mismo a las partes interesadas relevantes internas o externas que se requiera y deban tener conocimiento del mismo;

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

g) una vez que el incidente ha sido satisfactoriamente tratado, el cierre y registro formales del mismo;

h) llevar a cabo el análisis forense de seguridad de la información, según sea necesario (véase 5.28);

i) realizar un análisis post – incidente para identificar la causa raíz. Asegurar su documentación y comunicación de acuerdo a los procedimientos definidos (véase 5.27);

j) identificación y gestión de las vulnerabilidades o debilidades de la seguridad de la información incluyendo aquellas relacionadas con los controles que han causado, contribuido o fallado en la prevención del incidente.

Información adicional

La Norma ISO/IEC 27035 proporciona una guía adicional sobre la gestión de incidentes.

5.27 Aprender de los incidentes de seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

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

Propósito

Reducir la probabilidad o las consecuencias de los incidentes en el futuro.

Orientación

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

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

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

b) identificar los incidentes graves o recurrentes y sus causas para actualizar la evaluación de los riesgos de seguridad de la organización y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o las consecuencias de incidentes similares futuros. Mecanismos que permitan recoger, cuantificar y monitorizar la información sobre tipos de incidentes, volúmenes y costes;

c) mejorar la formación y concienciación de los usuarios (véase 6.3) proporcionando ejemplos de lo que puede ocurrir, de cómo responder ante esos incidentes y de cómo evitarlos en el futuro.

Información adicional

La serie de Normas ISO/IEC 27035 proporciona una guía adicional.

5.28 Recopilación de evidencias

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

La organización debería establecer e implementar procedimientos para la identificación, recogida, adquisición y preservación de evidencias relacionas con eventos de seguridad de la información.

Propósito

Asegurar una gestión de la evidencia consistente y efectiva de los incidentes de seguridad de la información con el fin de ejercer una acción disciplinaria y legal.

Orientación

Deberían desarrollarse procedimientos internos y seguirse a la hora de recopilar y presentar evidencias de los eventos de seguridad de la información con el fin de ejercer una acción disciplinaria y legal. Los requisitos de las diferentes jurisdicciones deberían tenerse en cuenta para maximizar las oportunidades de admisión de evidencias en las jurisdicciones relevantes.

Por lo general, estos procedimientos de gestión de la evidencia deberían proporcionar instrucciones para la identificación, recogida, adquisición y preservación de la evidencia de acuerdo con los diferentes tipos de medios de almacenamiento, dispositivos y condiciones de los mismos (por ejemplo, si están encendidos o apagados). La evidencia típicamente tiene que recogerse de modo que sea admisible en los juzgados nacionales correspondientes o en otro organismo disciplinario. Debería ser posible demostrar que:

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

b) las copias electrónicas de la evidencia son probablemente idénticas a las originales;

c) ningún sistema de información desde el cual la evidencia ha sido recogida estaba operativo en el momento del registro de la evidencia.

Cuando esté disponible, se debería proporcionar una certificación u otros medios relevantes que acrediten la cualificación del personal y los instrumentos utilizados, de modo que refuercen el valor de la evidencia preservada.

La evidencia digital puede transcender los límites de la organización y de su jurisdicción. En estos casos, se debería asegurar que la organización tiene derecho a recoger la información requerida como evidencia digital.

Información adicional

Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro de que se destruyan de forma intencional o accidental las evidencias necesarias antes de tomar conciencia de la gravedad del incidente. Es recomendable contar con asesoramiento legal o de aplicación de la ley desde el principio en cualquier acción legal que se esté considerando, así como el asesoramiento sobre las evidencias requeridas.

La Norma ISO/IEC 27037 proporciona definiciones y directrices para la identificación, recogida, adquisición y preservación de las evidencias digitales.

La serie de Normas ISO/IEC 27050 trata el descubrimiento electrónico, que implica el procesamiento electrónicamente de la información almacenada como evidencia.

5.29 Seguridad de la información durante la interrupción

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Continuidad	#Protección #Resiliencia

Control

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

Propósito

Proteger la información y otros activos asociados durante la interrupción.

Orientación

La organización debería definir los requisitos para adaptar los controles de seguridad de la información durante una interrupción. Los requisitos de seguridad de la información deberían incluirse en los procesos de gestión de la continuidad de negocio.

Los planes deberían desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener y restaurar la seguridad de la información de los procesos críticos de negocio tras una interrupción o fallo. La seguridad de la información debería restaurarse al nivel requerido y en los plazos requeridos.

La organización debería implementar y mantener:

a) los controles de seguridad de la información, que soportan los sistemas y las herramientas en los planes de continuidad de negocio y TIC;

b) los procesos que mantienen los controles existentes de seguridad de la información durante una interrupción;

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

Información adicional

En el contexto de la planificación de la continuidad de negocio y de la continuidad TIC, es necesario adaptar los requisitos de seguridad de la información dependiendo del tipo de interrupción, en comparación a las condiciones normales de operación. Como parte del análisis de impacto de negocio y la evaluación de riesgos realizados dentro de la gestión de la continuidad de negocio, las consecuencias de pérdida de confidencialidad e integridad de la información deberían considerarse y priorizarse además de la necesidad de mantener la disponibilidad.

Información sobre los sistemas de gestión de la continuidad de negocio puede encontrarse en las Normas ISO 22301 y ISO 22313. Una guía adicional sobre el análisis de impacto de negocio (BIA) puede encontrarse en la Norma ISO/TS 22317.

5.30 Preparación para las TIC para la continuidad del negocio

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Disponibilidad	#Responder	#Continuidad	#Resiliencia

Control

La resiliencia 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 una interrupción.

Orientación

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

Los requisitos de continuidad de las TIC son el resultado del análisis de impacto de negocio (BIA, business impact analysis). El proceso BIA debería utilizar tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo que resultan de la interrupción de las actividades de negocio que entregan productos y servicios. La magnitud y duración del impacto resultante debería utilizarse para identificar actividades prioritarias, a las cuales deberían asignarse un tiempo objetivo de recuperación (RTO, recovery time objetive). El BIA debería entonces determinar qué recursos son necesarios para soportar las actividades prioritarias. Un RTO debería también especificarse para estos recursos. Un subconjunto de estos recursos debería incluir los servicios TIC.

El BIA que involucra servicios TIC puede ampliarse para definir los requisitos de capacidad y rendimiento de los sistemas TIC y los puntos objetivo de recuperación (RPO, recovery point objetive) de la información necesarios para respaldar las actividades durante la interrupción.

En base a los resultaos del BIA y de la evaluación de riesgos relacionados con servicios 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 de negocio pueden comprometer una o más soluciones. Sobre la base de las estrategias, los planes deberían desarrollarse, implementarse y probarse para cumplir con el nivel de disponibilidad necesario de los servicios TIC y en los plazos de tiempo requeridos tras la interrupción o fallo de los procesos críticos.

La organización debería asegurar que:

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

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

   1) se evalúan regularmente mediante ejercicios y pruebas;

   2) se aprueban por la dirección;

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

   1) Especificaciones de rendimiento y capacidad para cumplir los requerimientos de continuidad de negocio y los objetivos como se especifica en el BIA;

   2) el RTO de cada servicio TIC prioritario y los procedimientos para restaurar estos componentes;

   3) el RPO de los recursos TIC prioritarios definido, así como la información y los procedimientos para restaurar la información.

Información adicional

La gestión de la continuidad de las TIC es una parte clave de los requisitos de continuidad del negocio relacionados con la disponibilidad para poder:

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

b) garantizar la continuidad de las actividades prioritarias con el apoyo de los servicios TIC necesarios;

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

Una guía adicional sobre preparación de las TIC para la continuidad de negocio puede encontrarse en la Norma ISO/IEC 27031.

Una guía adicional sobre los sistemas de gestión de la continuidad de negocio puede encontrarse en las Normas ISO 22301 y ISO 22313.

Una guía adicional sobre BIA puede encontrarse en la Norma ISO/TS 22317.

5.31 Identificación de requisitos legales, reglamentarios y contractuales

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_jurídico	#Gobernaza_y_Ecosistema #Protección

Control

Los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir estos requisitos deberían ser identificados, documentados y mantenerse actualizados.

Propósito

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

Orientación

General

Los requisitos externos, incluyendo los requisitos legales, estatutarios, reglamentarios o contractuales, deberían de tenerse en cuenta en:

a) el desarrollo de políticas y procedimientos de seguridad de la información;

b) el diseño, la implementación o el cambio de los controles de seguridad de la información;

c) la clasificación de la información y de otros activos asociados como parte del proceso que establece los requisitos de seguridad de la información para las necesidades internas o para los contratos con proveedores;

d) la realización de las evaluaciones de riesgos de seguridad de la información y la decisión de las actividades para el tratamiento de riesgos de seguridad de la información;

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

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

Legislación y regulaciones

La organización debería:

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

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

- realiza negocios en otros países;
- usa productos y servicios de otros países donde las leyes y los reglamentos podrían afectar a la organización;
- transfiere información a través de fronteras jurisdiccionales donde las leyes y los reglamentos podrían afectar a la organización.

c) revisar regularmente la legislación y normativa identificada con el fin de mantener actualizados los cambios e identificar nuevas legislaciones.

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

Criptografía

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

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

b) las restricciones a la importación y la exportación de *hardware* y *software* informático que esté diseñado para añadir funciones criptográficas al mismo;

c) las restricciones en el uso de la criptografía;

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

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

Se recomienda buscar asesoramiento legal para garantizar el cumplimiento de la legislación y los reglamentos pertinentes, especialmente cuando la información cifrada o las herramientas criptográficas se encuentran en los límites jurisdiccionales.

Contratos

Los requisitos contractuales relacionados con la seguridad de la información deberían incluirse en:

a) los contratos con clientes;

b) los contratos con proveedores (véase 5.20);

c) los contratos de seguros.

Información adicional

Ninguna información adicional.

5.32 Derechos de propiedad intelectual (DPI)

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_jurídico	#Gobernanza_y_Ecosistema

Control

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

Propósito

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

Orientación

Las siguientes directrices deberían tenerse en cuenta para proteger cualquier material que pueda ser considerado propiedad intelectual:

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

b) publicar procedimientos para el cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos *software* y de los productos de información;

c) adquirir *software* únicamente a través de fuentes reconocidas y de confianza para garantizar que no se infringen los derechos de autor;

d) mantener registros adecuados de los activos e identificar todos los activos que requieran la protección de los derechos de propiedad intelectual;

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

f) asegurar que no se exceden ni el número máximo de usuarios o ni de recursos permitidos por la licencia (como por ejemplo, unidades de procesamiento central (CPUs));

g) llevar a cabo comprobaciones de que sólo se instala *software* autorizado y productos licenciados;

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

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

j) cumplir los términos y las condiciones del *software* y de la información que se obtengan de redes públicas y fuentes externas;

k) no duplicar, convertir a otro formato o extraer de las grabaciones comerciales (video, audio) nada más que lo que permita la ley de derechos de autor o las licencias disponibles;

l) No copiar, parcial o totalmente, normas (por ejemplo, normas internacionales ISO/IEC), libros, artículos, informes u otros documentos, salvo lo que permita la ley de derechos de autor o las licencias disponibles.

Información adicional

Los derechos de propiedad intelectual incluyen los derechos de autor sobre el *software* o los documentos, los diseños, las marcas comerciales, las patentes y las licencias sobre el código fuente.

Los productos de *software* propietarios se suelen suministrar con un contrato de licencia que especifica los términos y condiciones de esta, por ejemplo, limitando el uso de los productos a unas máquinas específicas o limitando las copias exclusivamente a las de respaldo. Véase la serie de Normas ISO/IEC 19770 para los detalles sobre la gestión de activos.

Los datos pueden adquirirse de fuentes externas. Generalmente es el caso en el que los datos se obtienen bajo los términos de un acuerdo de intercambio de datos o un instrumento legal similar. Dicho acuerdo de intercambio de datos debería dejar claro qué procesamiento está permitido para los datos adquiridos. También se recomienda que se indique claramente la procedencia de los datos. Véase la Norma ISO/IEC 23751 para los detalles sobre los acuerdos para el intercambio de datos.

Los requisitos legales, estatutarios, reglamentarios y contractuales pueden imponer restricciones a la copia de material propietario. En particular, pueden exigir que sólo pueda utilizarse material desarrollado por la organización, que cuente con licencia o que haya sido suministrado por el desarrollador a la organización. La infracción de los derechos de autor puede desembocar en acciones legales que pueden incluir multas y procedimientos penales.

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

5.33 Protección de los registros

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_jurídico #Gestión_de_activos #Protección_de_la_información	#Defensa

Control

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

Propósito

Mejorar el cumplimiento de los requisitos legales, estatuarios, regulatorios y contractuales, así como las expectativas de la comunidad o de la sociedad relacionadas con la protección y disponibilidad de los registros.

Orientación

La organización debería seguir los siguientes pasos para proteger la autenticidad, la fiabilidad, la integridad y la usabilidad de los registros, y cuando el contexto de negocio y los requisitos para su gestión cambien en el tiempo:

a) emitir directrices sobre el almacenamiento, el manejo de la cadena de custodia y la eliminación de los registros, lo que incluye la prevención de la manipulación de los registros. Estas directrices deberían alinearse con la política específica de la organización sobre la gestión de registros y otros requisitos de los registros;

b) elaborar un plan de retención que defina los registros y el período de tiempo durante el cual deberían conservarse.

El sistema de almacenamiento y su manejo deberían garantizar la identificación de los registros y su período de retención teniendo en cuenta la legislación y los reglamentos nacionales o regionales, así como las expectativas de la comunidad o de la sociedad, si corresponde. El sistema debería permitir la destrucción adecuada de los registros tras ese periodo si dejan de ser necesarios para la organización.

En la decisión sobre la protección de los registros específicos de la organización debería considerarse su clasificación de seguridad de la información correspondiente de acuerdo al esquema de clasificación de la organización. Los registros deberían categorizarse en tipos de registros (por ejemplo, registros contables, registros de transacciones comerciales, registros de personal, registros de ámbito legal), cada uno con los 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 tal manera que los registros requeridos puedan recuperarse en un período de tiempo y formato aceptable, dependiendo de los requisitos que tienen que cumplirse.

Si se escogen soportes electrónicos de almacenamiento, deberían establecerse procedimientos que aseguren el acceso a los datos (tanto la legibilidad del soporte de almacenamiento como del formato) durante el periodo de retención con el fin de proteger contra la pérdida causada por futuros cambios de la tecnología. Cualquier clave criptográfica y programas asociados con archivos cifrados o firmas electrónicas deberían guardarse para permitir descifrar los registros durante el periodo de tiempo que éstos deberían ser retenidos (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. Debería considerarse la posibilidad de deterioro de los medios utilizados para el almacenamiento de los registros.

Información adicional

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

En la gestión de los registros, los metadatos son datos que describen el contexto, el contenido y la estructura de los registros, así como su gestión en el tiempo. Los metadatos son un componente esencial en 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 esenciales del negocio. Las leyes o reglamentos nacionales pueden establecer el período de tiempo y el contenido de los datos para la retención de la información. Se puede encontrar más información sobre la gestión de registros en la Norma ISO 15489.

5.34 Privacidad y protección de datos de carácter personal (DCP)

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Protección_de_la_información #Cumplimiento_jurídico	#Protección

Control

La organización debería identificar y cumplir los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal (DCP) de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.

Propósito

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

Orientación

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

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

El cumplimiento de estos procedimientos y toda la legislación y reglamentos relevantes relacionados con la preservación de la privacidad y protección de la PII requiere roles, responsabilidades y controles adecuados. A menudo, esto se logra mejor mediante la designación de una persona, como un responsable de privacidad, que debería proporcionar orientación al personal, a los proveedores de servicios y a otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que deberían seguirse.

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

Las medidas organizacionales y técnicas adecuadas para la protección de la PII deberían implementarse.

Información adicional

Varios países cuentan con legislación que impone controles sobre la recogida, el procesamiento, la transmisión y la eliminación de la PII. Dependiendo de la legislación nacional, estos controles pueden imponer obligaciones a quienes recopilan, procesan y difunden la PII y también pueden restringir la autoridad para transferir la PII a otros países.

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

La Norma ISO/IEC 29134 proporciona directrices para la evaluación de impacto relativa la protección de datos (EIPD) y aporta ejemplos de la estructura y contenidos de un informe PIA. Comparada con la Norma ISO/IEC 27005, esta norma está centrada en el procesamiento de la PII y es relevante para aquellas organizaciones que procesan la PII. Esta norma 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	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Garantía_de_seguridad_de_la_información	#Gobernanza_y_Ecosistema

Control

El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidos los procesos, la tecnología y las personas, debería revisarse de una forma independiente a intervalos planificados o siempre que se produzcan cambios significativos.

Propósito

Asegurar la idoneidad, la adecuación y la efectividad continuas del enfoque de la organización para gestionar la seguridad de la información.

Orientación

La organización debería tener procesos para llegar a cabo revisiones independientes.

La dirección debería planificar y encargar revisiones independientes periódicas. Las revisiones deberían incluir la evaluación de oportunidades de mejora y la necesidad de cambios del enfoque adoptado para la seguridad de la información, incluidas la política de seguridad de la información, las políticas específicas y otros controles.

Estas revisiones deberían llevarse a cabo por personas independientes del área bajo revisión (por ejemplo, el área de auditoría interna, un responsable independiente o una organización externa especializada en estas revisiones). Las personas encargadas de estas revisiones deberían tener las competencias adecuadas. La persona que realiza las revisiones no debería estar en la misma línea de autoridad para garantizar que tiene la independencia para hacer la evaluación.

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

Si las revisiones independientes identifican que el enfoque de la organización para la gestión de la seguridad de la información y su implantación es inadecuado [por ejemplo, si no se cumplen los objetivos y los requisitos documentados o bien éstos no cumplen con lo establecido para la seguridad de la información en la política de seguridad de la información y en las políticas específicas (véase 5.1)], la dirección debería iniciar acciones correctivas.

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

a) las leyes y normativa que afecta a la organización cambien;

b) incidentes significativos ocurren;

c) la organización comienza un nuevo negocio o cambia el negocio actual;

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

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

Información adicional

La Norma ISO/IEC 27007 y la Norma ISO/IEC TS 27008 proporcionan orientación para llevar a cabo revisiones independientes.

5.36 Cumplimiento de las políticas y normas de seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	##Cumplimiento_jurídico #Garantía_de_seguridad_de_la_información	#Gobernaza_y_Ecosistema

Control

Debería comprobarse periódicamente el cumplimiento con la política de seguridad de la información, las políticas específicas, las reglas y las normas de la organización.

Propósito

Asegurar que la seguridad de la información es implementada y operada de acuerdo con la política de seguridad de la información de la organización, con las políticas específicas, las reglas y las normas.

Orientación

Los directivos, los propietarios de la información o del producto o servicio deberían determinar cómo revisar que se cumplen los requisitos de seguridad de la información definidos en la política de seguridad de la información, en las políticas específicas, en las reglas, en las normas y en otros reglamentos aplicables. Se deberían considerar herramientas automáticas de medida y presentación para una revisión periódica eficiente.

Si como resultado de la revisión se identifica algún incumplimiento, los directivos o responsables deberían:

a) identificar las causas del incumplimiento;

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

c) implementar las acciones correctivas necesarias;

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

Los resultados de las revisiones y de las acciones correctivas realizadas por los directores, los propietarios de la información o del producto o servicio deberían ser registradas y los registros deberían ser mantenidos. Los directivos deberían informar de los resultados a las personas que realizaron las revisiones independientes (véase 5.35) cuando dicha revisión se realice en su área de responsabilidad.

Las acciones correctivas deberían completarse de manera oportuna según corresponda al riesgo. Si no se completa en la siguiente revisión planificada, el desarrollo debería abordarse al menos en esa revisión.

Información adicional

La monitorización operativa del uso del sistema está cubierta en los apartados 8.15, 8.16, 8.17.

5.37 Documentación de procedimientos operacionales

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión_de_activos #Seguridad_física #Seguridad_del_Sistema_y_de_la_red #Seguridad_de_las_aplicaciones #Configuración_segura #Gestión_de_identidad_y_de_acceso #Gestión_de_amenazas_y_de_vulnerabilidades #Continuidad #Gestión_de_eventos_de_seguridad_de_la_información	#Gobernanza_y_Ecosistema #Protección #Defensa

Control

Deberían documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.

Propósito

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

Orientación

Se deberían preparar procedimientos documentados para las actividades operacionales de la organización relacionadas con la seguridad de la información, como por ejemplo:

a) cuando la actividad tiene que ser realizada de la misma manera por muchas personas;

b) cuando la actividad se realiza con poca frecuencia y es probable que la próxima vez que se realice se haya olvidado el procedimiento;

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

d) antes de traspasar la actividad a nuevo personal.

Los procedimientos operacionales deberían especificar los siguientes aspectos:

a) las personas responsables;

b) la instalación y configuración seguras de los sistemas;

c) el tratamiento y la manipulación de la información, tanto automatizada como manual;

d) las copias de seguridad (véase 8.13) y la capacidad de recuperación;

e) los requisitos de programación, incluidas las interdependencias con otros sistemas;

f) instrucciones para el tratamiento de errores u otras condiciones excepcionales [por ejemplo, restricciones en el uso de programas de utilidades (véase 8.18)], que puedan surgir durante la ejecución del trabajo;

g) contactos de soporte y escalado, incluidos los contactos de soporte externo en caso de dificultades operativas o técnicas inesperadas;

h) instrucciones de manipulación de los soportes de almacenamiento (véanse 7.10 y 7.14);

i) procedimientos de reinicio y recuperación del sistema en caso de fallo de este;

j) la gestión de pistas de auditoría y de la información de registro del sistema (véanse 8.15 y 8.17) y los sistemas de monitorización por vídeo (véase 7.4);

k) procedimientos de monitorización tales como capacidad, rendimiento y seguridad (véanse 8.6 y 8.16);

l) instrucciones de mantenimiento.

La documentación sobre los procedimientos operacionales debería revisarse y actualizarse cuando sea necesario, y sus modificaciones deberían ser autorizadas. Y cuando sea técnicamente factible, los sistemas de información deberían gestionarse de forma coherente, utilizando los mismos procedimientos, herramientas y recursos.

Información adicional

Ninguna información adicional.

6 Controles de personas

6.1 Comprobación

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernanza_y_Ecosistema

Control

La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debería llevar a cabo antes de unirse a la organización y de forma continuada, de acuerdo con las leyes, reglamentos y éticas aplicables, y deberían ser proporcional a los requisitos empresariales, la clasificación de la información a la que se accederá y los riesgos percibidos.

Propósito

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

Orientación

Se debería realizar un proceso de investigación de antecedentes de todo el personal, tanto a tiempo completo, como a tiempo parcial y temporal. Cuando estas personas sean contratadas a través de proveedores de servicios, los requisitos sobre antecedentes deberían incluirse en los acuerdos contractuales entre la organización y dichos proveedores.

La información sobre todos los candidatos considerados para ocupar puestos en la organización debería ser recopilada y tratada teniendo en cuenta la legislación vigente en la jurisdicción correspondiente. En algunas jurisdicciones, se puede exigir legalmente a la organización que informe de antemano a los candidatos sobre las actividades de comprobación de antecedentes.

La verificación debería tener en consideración toda la legislación aplicable en materia de privacidad, protección de la información personal identificable y relativa a empleo, y cuando esté permitido, deberá incluir lo siguiente:

a) disponibilidad de referencias satisfactorias (por ejemplo, referencias de empresas y personas);

b) verificación del currículum vítae del solicitante (para comprobar que es completo y preciso);

c) confirmación de las cualificaciones académicas y profesionales presentadas;

d) comprobación independiente de la identificación (por ejemplo, pasaporte u otro documento aceptable expedido por las autoridades competentes);

e) una verificación más detallada, como la revisión crediticia o de antecedentes penales si el candidato asume una función crítica.

Cuando se contrata a una persona para un rol específico de seguridad de la información, la organización debería asegurarse de que el candidato:

a) tiene la competencia necesaria para desempeñar el rol de seguridad;

b) se puede confiar en él para asumir dicho perfil, especialmente si éste es crítico para la organización.

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

Los procedimientos deberían definir los criterios y las limitaciones de las comprobaciones (por ejemplo, quién es elegible para realizar la investigación de antecedentes, y cómo, cuándo y por qué se llevan a cabo las comprobaciones).

En situaciones en las que la verificación no pueda completarse a tiempo, deberán aplicarse controles paliativos hasta que la revisión haya finalizado, por ejemplo:

a) retraso en la incorporación;

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

c) incorporación con acceso reducido;

d) cese de la relación laboral.

Los controles de verificación deberían repetirse periódicamente para confirmar la idoneidad en todo momento del personal, en función de la importancia de la función de cada persona.

Información adicional

Ninguna información adicional.

6.2 Términos y condiciones de contratación

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Los acuerdos contractuales de empleo deberían indicar las responsabilidades del personal y de la organización en materia de seguridad de la información.

Propósito

Garantizar que el personal comprende sus responsabilidades en materia de seguridad de la información para las funciones para las que para las que son considerados.

Orientación

Las obligaciones contractuales del personal deberían tener en consideración la política de seguridad de la información de la organización y las políticas específicas relevantes. Además, pueden aclararse y establecerse los siguientes puntos:

a) el personal al que se le dé acceso a información confidencial debería firmar los acuerdos de confidencialidad o de no revelación de información de manera previa a darle acceso a dicha información y a otros activos asociados (véase 6.6);

b) las responsabilidades y derechos legales [por ejemplo, en relación con la legislación sobre derechos de autor o de protección de datos (véanse 5.32 y 5.34)];

c) las responsabilidades en materia de clasificación de la información y gestión de la información de la organización y de otros activos asociados, instalaciones de tratamiento de información y servicios de información manejados por el personal (véanse 5.9 a 5.13);

d) las responsabilidades de las partes interesadas del tratamiento de la información recibida;

e) las acciones que tienen que tomarse si el personal hace caso omiso de los requisitos de seguridad de la organización (véase 6.4).

Los roles y responsabilidades en materia de seguridad de la información deberían comunicarse a los candidatos durante el proceso previo a la contratación.

La organización debería asegurarse de que el personal acepta los términos y las condiciones relativas a la seguridad de la información. Estos términos y condiciones deberían ser apropiados para la naturaleza y el alcance del acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información. Los términos y condiciones relativos a la seguridad de la información deberán revisarse cuando cambie la legislación, los reglamentos, la política de seguridad de la información o las políticas específicas.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones de empleo deberían continuar durante un determinado periodo de tiempo después de la finalización de contratación (véase 6.5).

Información adicional

Se puede utilizar un código de conducta para establecer las responsabilidades del personal en materia de seguridad de la información en relación con la confidencialidad, la protección de la información personal identificable, la ética, el uso apropiado de la información de la organización y otros activos asociados, así como la buena reputación de la organización.

Se puede requerir a una parte externa, con la que esté asociado el personal proveedor, que celebre acuerdos contractuales en nombre de la persona contratada.

Si la organización no es una persona jurídica y no tiene empleados, el equivalente de acuerdo contractual y de los términos y condiciones pueden considerarse en la línea con las directrices de este control.

6.3 Concienciación, educación y formación en seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernanza_y_Ecosistema

Control

El personal de la organización y las partes interesadas pertinentes deberían recibir una adecuada concienciación, educación y formalización sobre la seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, y de las políticas y los procedimientos específicos, según corresponda a su puesto de trabajo.

Propósito

Garantizar que el personal y las partes interesadas relevantes conozcan y cumplan sus responsabilidades en materia de seguridad de la información.

Orientación

General

Debería establecerse un programa de concienciación, educación y capacitación en seguridad de la información de acuerdo con la política de seguridad de la información de la organización, con políticas específicas y con los procedimientos relevantes sobre seguridad de la información, teniendo en cuenta la información de la organización a proteger y los controles de seguridad de la información que se han implementado para proteger dicha información.

La concienciación, educación y capacitación en materia de seguridad de la información deberían tener lugar periódicamente. Una concienciación, educación y capacitación inicial puede ofrecerse al personal nuevo y a los que se trasladan 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 concienciación, educación o capacitación, para así comprobar la transferencia de conocimientos y la eficacia del programa específico.

Concienciación

Un programa de concienciación sobre la seguridad de la información debería tener como objetivo que el personal sea consciente de sus responsabilidades en materia de seguridad de la información y de los medios disponibles para cumplirlas.

El programa de concienciación debería planificarse teniendo en cuenta los roles del personal en la organización, incluido tanto el personal interno como externo (por ejemplo, consultores externos, personal de proveedores). Las actividades del programa de concienciación deberían programarse a lo largo del tiempo, preferiblemente con regularidad, de modo que las actividades se repitan y abarquen a nuevo personal. También debería basarse en las lecciones aprendidas de los incidentes de seguridad de la información.

El programa de concienciación debería incluir una serie de actividades de concienciación a través de canales físicos o virtuales adecuados, como campañas, folletos, carteles, boletines, sitios web, sesiones o reuniones informativas, módulos de aprendizaje electrónico y correos electrónicos.

La concienciación sobre la seguridad de la información debería abarcar aspectos generales como:

a) el compromiso de la dirección con la seguridad de la información en toda la organización;

b) las necesidades de familiarización y cumplimiento de las normas y obligaciones aplicables en materia de seguridad de la información, teniendo en cuenta la política de seguridad de la información y otras políticas específicas, normas, legislación, estatutos, reglamentos, contratos y acuerdos;

c) responsabilidad personal por las propias acciones e inacciones, y responsabilidades generales para la seguridad o protección de la información perteneciente a la organización y a las partes interesadas;

d) procedimientos básicos de seguridad de la información [por ejemplo, notificación de eventos de seguridad de la información (6.8)] y controles básicos [por ejemplo, seguridad de contraseñas (5.17)];

e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre materia de seguridad de la información, incluido más material de concienciación sobre seguridad de la información.

Educación y capacitación

La organización debería identificar, preparar e implementar un plan de formación adecuado para los equipos técnicos cuyos roles requieran destrezas 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 para ello, la organización debería tomar medidas para que las adquieran.

El programa de educación y capacitación debería considerar distintas formas [por ejemplo, conferencias o autoaprendizaje, formación en el puesto de trabajo a cargo de expertos o consultores, rotación del personal para seguir diferentes actividades, contratación de personal ya cualificado, o subcontratación de consultores]. Puede utilizar diferentes medios de impartición, como la formación presencial, a distancia, a través de Internet, a su propio ritmo, etc. El personal técnico debería mantener al día sus conocimientos suscribiéndose a boletines y revistas o asistiendo a conferencias y eventos destinados a la mejora técnica y profesional.

Información adicional

A la hora de elaborar un programa de concienciación, es importante no sólo centrarse en el "qué" y el "cómo", sino también en el "por qué", siempre que sea posible. Es importante que el personal comprenda el objetivo de la seguridad de la información y sus posibles efectos, positivos y negativos, de su propio comportamiento en la organización.

La concienciación, la educación y la capacitación en materia de seguridad de la información pueden formar parte de otras actividades, o llevarse a cabo en colaboración con ellas, como por ejemplo, en la formación en gestión general de la información, TIC, seguridad o privacidad.

6.4 Proceso disciplinario

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad_de_los_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Debería existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertinentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.

Propósito

Garantizar que el personal y otras partes interesadas relevantes comprendan las consecuencias de la violación de la política de seguridad de la información, para disuadirlas y para tratarles adecuadamente en caso de cometer infracción.

Orientación

El proceso disciplinario no debería iniciarse sin la verificación previa de que se ha producido una infracción de la política de seguridad de la información (véase 5.28).

El proceso disciplinario formal debería prever una respuesta gradual que tenga en cuenta factores como:

a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad de la infracción y sus consecuencias;

b) si la infracción ha sido intencionada (dolosa) o no intencionada (accidental);

c) si se trata o no de una primera infracción o de una reincidencia;

d) si el infractor recibió o no la formación adecuada.

La respuesta debería tener en consideración los requisitos legales, estatutarios, reglamentarios, contractuales y empresariales relevantes, así como otros factores necesarios. El proceso disciplinario también debería ser disuasorio para evitar que el personal y otras partes interesadas violen la política de seguridad de la información, otras políticas específicas y los procedimientos de seguridad de la información. Las violaciones deliberadas de la política de seguridad de la información pueden requerir medidas inmediatas.

Información adicional

Siempre que sea posible, la identidad de las personas sujetas a medidas disciplinarias debería protegerse de acuerdo con los requisitos aplicables.

Cuando las personas demuestren un comportamiento excelente en relación con la seguridad de la información, podrían ser recompensados para promover la seguridad de la información y fomentar el buen comportamiento.

6.5 Responsabilidades ante la finalización o cambio

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos #Gestión_de_activos	#Gobernanza_y_Ecosistema

Control

Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cese o cambio de empleo se deberían definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.

Propósito

Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos.

Orientación

El proceso para gestionar la terminación o cambio de empleo debería definir qué responsabilidades y obligaciones sobre seguridad de la información deberían permanecer válidos después de la terminación o cambio. Esto puede incluir la confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos, así como responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (véase 6.6). Las responsabilidades y obligaciones que sigan siendo válidas tras la finalización del empleo o del contrato deberían figurar en los términos y condiciones del empleo de la persona (véase 6.2), su contrato o en los acuerdos establecidos. Otros contratos o acuerdos que se prolonguen durante un periodo determinado tras la finalización de la relación laboral también pueden incluir responsabilidades en materia de seguridad de la información.

Los cambios de responsabilidad o de empleo deberían gestionarse como el cese de la responsabilidad o empleo actual combinado con el inicio de la nueva responsabilidad o empleo.

Los roles y responsabilidades en materia de seguridad de la información de cualquier persona que abandone o cambie de puesto de trabajo deberían identificarse y transferirse a otra persona.

Debería establecerse un proceso para la comunicación de los cambios y de los procedimientos operacionales al personal, a otras partes interesadas (por ejemplo, a clientes y proveedores).

El proceso de finalización o cambio de empleo debería aplicarse también al personal externo (es decir, a los proveedores) cuando se produzca una finalización del contrato o del puesto de trabajo de dicho personal con la organización, o cuando se produzca un cambio de puesto de trabajo dentro de la organización.

Información adicional

En muchas organizaciones, el departamento de recursos humanos suele tener la responsabilidad del proceso completo de finalización del contrato, y trabaja conjuntamente con el supervisor que deja su puesto para gestionar los aspectos de seguridad de la información de los procedimientos relevantes. En el caso del personal proporcionado mediante una tercera parte (por ejemplo, a través de un proveedor), este proceso de finalización será gestionado por ésta de acuerdo con el contrato entre la organización y la tercera parte.

6.6 Acuerdos de confidencialidad o no divulgación

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_de_los_recursos_humanos #Protección_de_la_información #Relación_con_los_proveedores	#Gobernanza_y_Ecosistema

Control

Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deberían ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

Propósito

Mantener la confidencialidad de la información a la que tiene acceso el personal o partes externas.

Orientación

Los acuerdos de confidencialidad o de no revelación deberían cumplir el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no revelación son aplicables tanto a las partes interesadas como al personal de la organización. Basándose en 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 de los acuerdos de confidencialidad o no revelación, deberían tenerse en cuenta los siguientes elementos:

a) una definición de la información a proteger (por ejemplo, información confidencial);

b) la duración prevista de un acuerdo, incluidos los casos en los que puede ser necesario mantener confidencialidad indefinidamente o hasta que la información pase a ser de dominio público;

c) las acciones necesarias cuando se pone fin a un acuerdo;

d) las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información;

e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y su relación con la protección de la información confidencial;

f) el uso permitido de la información confidencial y los derechos del firmante a utilizar la información;

g) el derecho a auditar y supervisar las actividades que impliquen información confidencial en circunstancias altamente sensibles;

h) el proceso de notificación y aviso de la revelación no autorizada o fuga de información confidencial;

i) los términos en los que la información debería ser devuelta o destruida en la finalización del acuerdo;

j) las acciones para llevar a cabo en caso de incumplimiento del acuerdo.

La organización debería tener en consideración el cumplimiento de los acuerdos de confidencialidad y no revelación para la jurisdicción a la que se aplican (véanse 5.31, 5.32, 5.33, 5.34).

Los requisitos de los acuerdos de confidencialidad y no revelación deberían revisarse periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

Información adicional

Los acuerdos de confidencialidad y no revelación protegen la información de la organización e informan a los firmantes de su responsabilidad de proteger, utilizar y revelar la información de forma responsable y autorizada.

6.7 Teletrabajo

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información #Seguridad_física #Seguridad_del_Sistema_y_de_la_red	#Protección

Control

Se deberían implementar medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.

Propósito

Garantizar la seguridad de la información cuando el personal trabaja de manera remota.

Orientación

Desde una ubicación de fuera de los locales de la organización, accediendo a la información ya sea en papel o electrónicamente a través de equipos TIC. Los entornos de trabajo remoto incluyen aquellos relativos a "teletrabajo", "trabajo a distancia", "lugar de trabajo flexible", "entornos de trabajo virtuales" y "mantenimiento a distancia".

NOTA Es posible que no todas las recomendaciones de esta guía puedan aplicarse debido a la legislación local y reglamentos de las distintas jurisdicciones.

Las organizaciones que permiten actividades de trabajo de manera remota deberían instrumentar una política específica que defina las condiciones y restricciones sobre el trabajo remoto. Cuando se considere aplicable, se deberían tener en consideración los siguientes aspectos:

a) la seguridad física existente o propuesta del lugar de trabajo de manera remota, teniendo en cuenta la seguridad física del lugar y el entorno local, incluidas las diferentes jurisdicciones en las que se encuentre el personal;

b) normas y mecanismos de seguridad para el entorno físico remoto, tales como archivadores con cerradura, transporte seguro entre ubicaciones y normas para el acceso remoto, escritorio despejado, impresión y eliminación de información y otros activos asociados, y notificación de eventos de seguridad de la información (véase 6.8);

c) los entornos físicos de trabajo de manera remoto previstos;

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 va a acceder y transmitir a través del enlace de comunicación, así como la sensibilidad de los sistemas y aplicaciones;

e) el uso de acceso remoto, como el acceso a escritorios virtuales que admiten el procesamiento y almacenamiento de información en equipos de propiedad privada;

f) la amenaza de acceso no autorizado a información o recursos por parte de otras personas que se encuentren en el lugar de trabajo remoto (por ejemplo, familiares y amigos);

g) la amenaza de acceso no autorizado a información o recursos por parte de otras personas en lugares públicos;

h) el uso de redes domésticas y redes públicas, y los requisitos o restricciones sobre la configuración de los servicios de redes inalámbricas;

i) el uso de medidas de seguridad, como cortafuegos y protección contra programas maliciosos;

j) mecanismos seguros para desplegar e inicializar sistemas de manera remota;

k) mecanismos seguros para la autenticación y establecimiento de privilegios de acceso teniendo en cuenta la vulnerabilidad de los mecanismos de autenticación de factor único cuando 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 mobiliario de almacenamiento adecuados para las actividades de trabajo a distancia, cuando no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;

b) una definición de los trabajos permitidos, la clasificación de la información que se puede manejar y los sistemas y servicios internos a los que está autorizado a acceder el trabajador a distancia;

c) la provisión de la formación de las personas que trabajan a distancia y de las que les prestan apoyo. Esta formación debería incluir cómo realizar los procesos de negocio de forma segura mientras se trabaja a distancia;

d) el suministro de los equipos de comunicación adecuados, incluidos métodos para proteger el acceso remoto, como los requisitos de bloqueo de la pantalla del dispositivo y temporizadores de inactividad; la habilitación del seguimiento de la ubicación del dispositivo; la instalación de funciones de borrado a distancia;

e) seguridad física;

f) normas y directrices sobre el acceso de familiares y visitantes a los equipos y la información;

g) la provisión de soporte y mantenimiento de *hardware* y *software*;

h) la provisión de seguros;

i) los procedimientos de copia de seguridad y continuidad del negocio;

j) la auditoría y la supervisión de la seguridad;

k) la revocación de la autorización y de los derechos de acceso y la devolución del equipo cuando finalicen las actividades de trabajo a distancia.

Información adicional

Ninguna información adicional.

6.8 Notificación de los eventos de seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	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 notifique a tiempo eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.

Propósito

Proporcionar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que puedan ser identificados por el personal.

Orientación

Todo el personal y los usuarios deberían ser conscientes de su responsabilidad de notificar los eventos de seguridad de la información lo antes posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información.

También deberían conocer el procedimiento para notificar eventos de seguridad de la información y el punto de contacto al que deberían notificarse. El mecanismo de notificación debería ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, brechas y vulnerabilidades.

Las situaciones que deberían tenerse en cuenta para la notificación de eventos de seguridad de la información incluyen:

a) controles de seguridad de la información ineficaces;

b) brechas en las expectativas de confidencialidad, integridad o disponibilidad de la información;

c) errores humanos;

d) incumplimiento de la política de seguridad de la información, otras políticas específicas o normas aplicables;

e) brechas de las medidas de seguridad física;

f) cambios en el sistema que no hayan pasado por el proceso de gestión de cambios;

g) fallos de funcionamiento u otros comportamientos anómalos del *software* o *hardware* del sistema;

h) infracciones de acceso;

i) vulnerabilidades;

j) sospecha de infección por código malicioso.

Se debería aconsejar al personal y a los usuarios que no intenten probar las presuntas vulnerabilidades de la seguridad de la información. Probar vulnerabilidades puede interpretarse como un potencial uso indebido del sistema y también puede causar daños al sistema o al servicio de información, y puede corromper u ocultar pruebas digitales. En última instancia, esto puede dar lugar a responsabilidad legal para la persona que realiza las pruebas.

Información adicional

Para más información, consulte la serie de Normas ISO/IEC 27035.

7 Controles físicos

7.1 Perímetro de seguridad física

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Se deberían definir y utilizar perímetros de seguridad para proteger áreas que contengan información y otros activos asociados.

Propósito

Impedir el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados.

Orientación

Las siguientes directrices deberían ser consideradas e implementadas 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) disponer de perímetros físicamente sólidos para un edificio o emplazamiento que contenga instalaciones de tratamiento de la información (es decir, no debería haber huecos en el perímetro ni zonas en las que pueda producirse fácilmente una intrusión). Los tejados, paredes, techos y suelos exteriores del lugar deberían ser de construcción sólida y todas las puertas exteriores deberían estar adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, rejas, alarmas, cerraduras). Las puertas y ventanas deberían cerrarse con llave cuando estén desatendidas y debería considerarse la posibilidad de instalar protecciones externas en las ventanas, especialmente a nivel del suelo; también deberían considerarse los puntos de ventilación;

c) todas las puertas del perímetro de seguridad que actúen como cortafuegos deberían estar dotadas de un sistema de alarma, control y prueba junto con las paredes, para establecer el nivel requerido de resistencia, de acuerdo con las normas adecuadas. Deberían funcionar a prueba de fallos.

Información adicional

La protección física puede lograrse creando una o más barreras físicas alrededor de los locales de la organización y las instalaciones de procesamiento de la información.

Una zona segura puede ser una oficina con cerradura o varias salas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarias barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. La organización debería considerar la posibilidad de tener medidas de seguridad física que puedan reforzarse en situaciones de mayor amenaza.

7.2 Controles físicos de entrada

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_identidad_y_de_acceso	#Protección

Control

Las áreas seguras deberían estar protegidas por controles de entrada y puntos de acceso adecuados.

Propósito

Garantizar que sólo se produce el acceso físico autorizado a la información de la organización y a otros activos asociados.

Orientación

General

Los puntos de acceso, como las zonas de entrega y carga y otros puntos en los que pueden entrar personas no autorizadas, deberían controlarse y, si es posible, aislarse de las instalaciones de tratamiento de la información para evitar accesos no autorizados.

Deberían considerarse las siguientes directrices:

a) restringir el acceso a las instalaciones y edificios únicamente al personal autorizado. El proceso de gestión de los derechos de acceso a las zonas físicas debería incluir la concesión, revisión periódica, actualización y revocación de las autorizaciones (véase 5.18);

b) mantener y supervisar de forma 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 sensible de autenticación;

c) establecer e implementar un proceso y los mecanismos técnicos para la gestión del acceso a las zonas en las que se procesa o almacena información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Debería considerarse la posibilidad de utilizar puertas de doble seguridad para acceder a las zonas sensibles;

d) establecer una zona de recepción vigilada por personal, u otros medios para controlar el acceso físico al recinto o edificio;

e) inspeccionar y examinar los efectos personales del personal y de las partes interesadas a la entrada y a la salida;

NOTA Puede existir legislación y normativa local sobre la posibilidad de inspeccionar los efectos personales.

f) exigir a todo el personal y a las partes interesadas que lleven algún tipo de identificación visible y que avisen inmediatamente al personal de seguridad si se encuentran con visitantes sin escolta o con alguien que no lleve una identificación visible. Para identificar mejor a los empleados fijos, los proveedores y los visitantes, debería considerarse la posibilidad de utilizar distintivos fácilmente diferenciables;

g) conceder al personal de los proveedores un acceso restringido a las zonas seguras o a las instalaciones de tratamiento de la información sólo cuando sea necesario. Este acceso debería ser autorizado y supervisado;

h) prestar especial atención a la seguridad del acceso físico en el caso de edificios que alberguen activos para múltiples organizaciones;

i) diseñar las medidas de seguridad física de modo que puedan reforzarse cuando aumente la probabilidad de incidentes físicos;

j) proteger otros puntos de entrada de accesos no autorizados, como las salidas de emergencia;

k) establecer un proceso de gestión de llaves que garantice la gestión de las llaves físicas o la información de autenticación (por ejemplo, códigos de cerraduras, cerraduras de combinación de oficinas, salas e instalaciones como armarios de llaves) y que garantice un libro de registro o una auditoría anual de llaves y que se controle el acceso a las llaves físicas o a la información de autenticación (véase 5.17 para más orientación sobre la información de autenticación).

Visitantes

Deberían tenerse en cuenta las siguientes directrices:

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) conceder acceso a los visitantes únicamente para fines específicos y autorizados y con instrucciones sobre los requisitos de seguridad de la zona y sobre los procedimientos de emergencia;

d) supervisar a todos los visitantes, a menos que se conceda una excepción explícita.

Zonas de entrega y carga y material entrante

Deberán tenerse en cuenta las siguientes directrices:

a) restringir el acceso a las zonas de entrega y carga desde el exterior del edificio al personal identificado y autorizado;

b) diseñar las zonas de entrega y carga de modo que las entregas puedan cargarse y descargarse sin que el personal de entrega acceda sin autorización a otras partes del edificio;

c) asegurar las puertas exteriores de las zonas de entrega y carga cuando se abran las puertas de las zonas restringidas;

d) inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que salgan de las zonas de entrega y carga;

e) registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos (véanse 5.9 y 7.10) a la entrada de las instalaciones;

f) separar físicamente los envíos entrantes y salientes, siempre que sea posible;

g) inspeccionar las entregas entrantes en busca de indicios de manipulación en el camino. Si se descubren manipulaciones, debería informarse inmediatamente de ellas.

Información adicional

Ninguna información adicional.

7.3 Seguridad de oficinas, despachos y recursos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Para las oficinas, despachos y recursos, se debería diseñar y aplicar la seguridad física.

Propósito

Impedir el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados en oficinas, salas e instalaciones.

Orientación

Deberían tenerse en cuenta las siguientes directrices para proteger oficinas, salas e instalaciones:

a) ubicar las instalaciones críticas para evitar el acceso del público;

b) cuando proceda, asegurarse de que los edificios sean discretos y den una indicación mínima de su finalidad, sin signos evidentes, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de la información;

c) configurar las instalaciones para evitar que la información o las actividades confidenciales sean visibles y audibles desde el exterior. También debería considerarse, en su caso, el blindaje electromagnético;

d) no poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen la ubicación de las instalaciones de tratamiento de la información confidencial.

Información adicional

Ninguna información adicional.

7.4 Monitorización de la seguridad física

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección #Defensa

Control

Las instalaciones deberían ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.

Propósito

Detectar e impedir el acceso físico no autorizado.

Guía

Los locales físicos deberían controlarse mediante sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de vídeo vigilancia, como televisión en circuito cerrado, y programas informáticos de gestión de la información sobre seguridad física, ya sean gestionados internamente o por un proveedor de servicios de vigilancia.

El acceso a los edificios que albergan sistemas críticos debería vigilarse continuamente para detectar accesos no autorizados o comportamientos sospechosos mediante:

a) la instalación de sistemas de vídeo vigilancia, como circuitos cerrados de televisión, para ver y grabar el acceso a las zonas sensibles dentro y fuera de los locales de una organización;

b) la instalación, de acuerdo con las normas aplicables relevantes, y la comprobación periódica de detectores de contacto, sonido o movimiento para activar una alarma de intrusión, como, por ejemplo:

   1) instalación de detectores de contacto que activen una alarma cuando se haga o se rompa un contacto en cualquier lugar donde se pueda hacer o romper un contacto (como ventanas y puertas y debajo de objetos) para ser utilizados como alarma de pánico;

   2) detectores de movimiento basados en tecnología de infrarrojos que activan una alarma cuando un objeto pasa por su campo de visión;

   3) instalación de sensores sensibles al ruido de rotura de cristales que puedan utilizarse para activar una alarma que alerte al personal de seguridad;

c) utilizar esas alarmas para cubrir todas las puertas exteriores y ventanas accesibles. Las zonas desocupadas deberían tener alarma en todo momento; también debería proporcionarse cobertura a otras zonas (por ejemplo, salas de ordenadores o de comunicaciones).

El diseño de los sistemas de vigilancia debería ser confidencial, ya que su revelación puede facilitar accesos no detectados.

Los sistemas de vigilancia deberían protegerse del acceso no autorizado para evitar que personas no autorizadas accedan a la información de vigilancia, como las imágenes de vídeo, o que los sistemas se desactiven a distancia.

El panel de control del sistema de alarma debería estar situado en una zona de alarma y, en el caso de las alarmas de seguridad, en un lugar que permita una salida fácil a 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, sobre todo si sus componentes funcionan con pilas.

Cualquier mecanismo de supervisión y grabación debería utilizarse teniendo en cuenta las leyes y normativas locales, incluida la legislación sobre protección de datos e información personal identificable, especialmente en lo relativo a la supervisión del personal y los periodos de conservación de los vídeos grabados.

Información adicional

Ninguna información adicional.

7.5 Protección contra las amenazas externas y ambientales

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Se debería diseñar e implementar una protección a las infraestructuras contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionadas o no.

Propósito

Prevenir o reducir las consecuencias de sucesos originados por amenazas físicas y medioambientales.

Orientación

Las evaluaciones de riesgos para identificar las consecuencias potenciales de las amenazas físicas y medioambientales deberían realizarse antes de comenzar las operaciones críticas en un emplazamiento físico, y a intervalos regulares. Deberían aplicarse las salvaguardias necesarias y vigilarse los cambios en las amenazas. Debería obtenerse asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y medioambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, residuos tóxicos, emisiones medioambientales y otras formas de catástrofes naturales o provocadas por el hombre.

La ubicación física de los locales y su construcción deberían tener en consideración:

a) la topografía local, como la elevación adecuada, las masas de agua y las fallas tectónicas;

b) las amenazas urbanas, como los lugares proclives a atraer disturbios políticos, actividades delictivas o atentados terroristas.

Basándose en los resultados de la evaluación de riesgos, deberían identificarse las amenazas físicas y medioambientales pertinentes y considerarse los controles adecuados en los siguientes contextos, a modo de ejemplo:

a) incendio: instalación y configuración de sistemas capaces de detectar incendios en una fase temprana para enviar alarmas o activar sistemas de extinción de incendios con el fin de evitar daños por incendio a los medios de almacenamiento y a los sistemas de procesamiento de la información relacionados. La extinción de incendios debería realizarse utilizando la sustancia más adecuada en relación con el entorno circundante (por ejemplo, gas en espacios confinados);

b) inundación: instalación de sistemas capaces de detectar inundaciones en una fase temprana bajo los suelos de las zonas que contengan medios de almacenamiento o sistemas de tratamiento de la información. En caso de inundación, debería disponerse de bombas de agua o medios equivalentes;

c) sobretensiones eléctricas: adopción de sistemas capaces de proteger los sistemas de información tanto del servidor como del cliente contra sobretensiones eléctricas o sucesos similares para minimizar las consecuencias de tales sucesos;

d) explosivos y armas: realizar inspecciones aleatorias para detectar la presencia de explosivos o armas en el personal, los vehículos o los bienes que entren en las instalaciones de tratamiento de la información sensible.

Información adicional

Las cajas fuertes u otras formas de instalaciones de almacenamiento seguro pueden proteger la información almacenada en ellas contra catástrofes como incendios, terremotos, inundaciones o explosiones.

Las organizaciones pueden tener en consideración los conceptos de prevención de la delincuencia mediante el diseño de los controles para asegurar su entorno y reducir las amenazas urbanas. Por ejemplo, en lugar de utilizar bolardos, estatuas o elementos acuáticos pueden servir tanto de elemento decorativo como de barrera física.

7.6 El trabajo en áreas seguras

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Se debería diseñar e implementar procedimientos para trabajar en las áreas seguras.

Propósito

Proteger la información y otros activos asociados en áreas seguras de daños e interferencias no autorizadas por parte del personal que trabaja en dichas áreas.

Orientación

Las medidas de seguridad para trabajar en áreas seguras deberían aplicarse a todo el personal y abarcar todas las actividades que tengan lugar en el área segura.

Se deberían considerar las siguientes directrices:

a) informar al personal únicamente de la existencia de un área segura, o de las actividades que se desarrollan en ella, en función de la necesidad de conocerla;

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 desocupadas;

d) no permitir equipos fotográficos, de vídeo, de audio u otros equipos de grabación, como cámaras en dispositivos finales de usuario, a menos que esté autorizado;

e) controlar adecuadamente el transporte y el uso de dispositivos finales de usuario en zonas seguras;

f) publicar los procedimientos de emergencia de manera fácilmente visible o accesible.

Información adicional

Ninguna información adicional.

7.7 Puesto de trabajo despejado y pantalla limpia

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física	#Protección

Control

Deberían definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información.

Propósito

Para reducir los riesgos de acceso no autorizado, pérdida y daño de información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario laboral normal.

Orientación

La organización debería establecer y comunicar a todas las partes interesadas pertinentes una política específica sobre puesto de trabajo despejado y pantalla limpia.

Se deberían considerar las siguientes directrices:

a) guardar bajo llave información de negocio sensible o crítica (por ejemplo, en papel o en soportes de almacenamiento electrónico) (idealmente en una caja fuerte, armario u otro tipo de mueble de seguridad) cuando no sea necesario, especialmente cuando la oficina está desocupada;

b) proteger los dispositivos finales de usuario mediante candado o anclaje con llave u otros medios de seguridad cuando no estén en uso o estén desatendidos;

c) dejar los dispositivos finales de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando están desatendidos. Todos los equipos y sistemas deberían configurarse con una función de tiempo de espera o cierre de sesión automático;

d) hacer que el remitente recoja inmediatamente los resultados en las impresoras o dispositivos multifunción. Considerar el uso de impresoras con función de autenticación, de tal manera que los remitentes sean los únicos que puedan obtener sus impresiones, y solo cuando estén de pie junto a la impresora;

e) almacenar de forma segura documentos y soportes de almacenamiento extraíbles que contengan información sensible y, cuando ya no sea necesario, desecharlos utilizando mecanismos de eliminación seguros;

f) establecer y comunicar normas y orientaciones para la configuración de ventanas emergentes en las pantallas (por ejemplo, desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, uso compartido de pantalla o en una zona pública);

g) borrar información sensible o crítica de las pizarras y otros tipos de pantallas cuando ya no sea necesario.

La organización debería contar con procedimientos para desocupar unas instalaciones que incluyan la realización de una inspección física final antes de irse, para garantizar que los activos de la organización no se queden atrás (por ejemplo, documentos caídos detrás de cajones o muebles).

Información adicional

Ninguna información adicional.

7.8 Emplazamiento y protección de equipos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_Física #Gestión_de_activos	#Protección

Control

Los equipos deberían situarse de forma protegida y segura.

Propósito

Reducir los riesgos derivados de amenazas físicas y medioambientales, así como de accesos no autorizados y daños.

Orientación

Se deberían considerar las siguientes directrices para proteger los equipos:

a) situar los equipos de forma que se reduzca al mínimo el acceso innecesario a las zonas de trabajo y se evite el acceso no autorizado;

b) situar cuidadosamente las instalaciones de tratamiento de la información que manejan datos sensibles para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso;

c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales como, por ejemplo, robo, fuego, explosivos, humo, agua (o fallo de suministro de agua), polvo, vibración, agentes químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiaciones electromagnéticas y vandalismo;

d) establecer directrices para comer, beber y fumar cerca de las instalaciones de tratamiento de la información;

e) controlar las condiciones ambientales, como la temperatura y la humedad, para detectar condiciones que puedan afectar negativamente al funcionamiento de las instalaciones de tratamiento de la información;

f) aplicar protección contra rayos a todos los edificios e instalar filtros de protección contra rayos en todas las entradas de alimentación eléctrica y líneas de comunicaciones;

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 tratamiento de la información gestionadas por la organización de las no gestionadas por la organización.

Información adicional

Ninguna información adicional.

7.9 Seguridad de los equipos fuera de las instalaciones

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Los activos fuera de las instalaciones deberían estar protegidos.

Propósito

Evitar la pérdida, daño, robo o compromiso de dispositivos fuera de las instalaciones e interrupción de las operaciones de la organización.

Orientación

Se necesita proteger cualquier dispositivo utilizado fuera de las instalaciones de la organización que almacene o procese información (por ejemplo, dispositivo móvil), incluidos los dispositivos propiedad de la organización y los dispositivos de propiedad privada, utilizados en nombre de la organización [Bring Your Own Device (BYOD)/ "Traiga Su Propio Dispositivo"]. El uso de estos dispositivos debería ser autorizado por la dirección.

Se deberían considerar las siguientes pautas para la protección de dispositivos que almacenan o procesan información fuera de las instalaciones de la organización:

a) no dejar desatendidos en lugares públicos y no seguros los equipos y soportes de almacenamiento que se lleven fuera de las instalaciones;

b) respetar las instrucciones del fabricante para proteger el equipo en todo momento (por ejemplo, protección contra la exposición a campos electromagnéticos fuertes, agua, calor, humedad, polvo);

c) cuando se transfieran equipos fuera de las instalaciones entre diferentes personas o partes interesadas, mantener un registro que defina la cadena de custodia de los equipos, incluyendo al menos los nombres y organizaciones de los responsables de los equipos. La información que no deba transferirse con el activo debería ser eliminada de forma segura antes de la transferencia;

d) cuando sea necesario y práctico, exigir autorización para retirar el equipo y los medios de comunicación de los locales de la organización y llevar un registro de dichos traslados a fin de mantener una pista de auditoría (véase 5.14);

e) protección contra la visualización de información en un dispositivo (por ejemplo, móvil o portátil) en el transporte público, y los riesgos asociados con el “shoulder surfing” (<<mirar por encima del hombro>>);

f) implementar el seguimiento de la ubicación y la posibilidad de borrar a distancia los dispositivos.

La instalación permanente de equipos fuera de las instalaciones de la organización [como antenas y cajeros automáticos (Automated Teller Machines (ATMs)] puede estar sujeta a un mayor riesgo de daños, robos o escuchas. Estos riesgos pueden variar considerablemente entre lugares y deberían tenerse en cuenta para determinar las medidas más adecuadas. Se deberían considerar las siguientes pautas al ubicar este equipo fuera de las instalaciones de la organización:

a) monitorización de la seguridad física (véase 7.4);

b) protección contra amenazas físicas y medioambientales (véase 7.5);

c) controles de acceso físico y a prueba de manipulaciones;

d) controles de acceso lógico.

Información adicional

Puede encontrar más información sobre otros aspectos de la protección de equipos de almacenamiento y procesamiento de información y dispositivos finales de usuario en los apartados 8.1 y 6.7.

7.10 Soportes de almacenamiento

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Los soportes de almacenamiento deberían gestionarse durante todo su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

Propósito

Garantizar únicamente la divulgación, modificación, eliminación o destrucción autorizadas de la información contenida en los soportes de almacenamiento.

Orientación

Soportes de almacenamiento extraíbles

Se deberían tener en cuenta las siguientes directrices para la gestión de medios de almacenamiento extraíbles:

a) establecer una política específica sobre la gestión de soportes de almacenamiento extraíbles y comunicar dicha política específica a cualquier persona que utilice o manipule soportes de almacenamiento extraíbles;

b) cuando sea necesario y práctico, exigir autorización para que los soportes de almacenamiento se retiren de la organización y mantener un registro de dichas eliminaciones a fin de mantener una pista de auditoría;

c) almacenar todos los soportes de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones del fabricante;

d) si la confidencialidad o integridad de la información son consideraciones importantes, utilizar técnicas criptográficas para proteger la información en soporte de almacenamiento extraíbles;

e) mitigar el riesgo de que los soportes de almacenamiento se degraden mientras la información almacenada sigue siendo necesaria, transfiriendo la información a soportes de almacenamiento nuevos antes de que se vuelva ilegible;

f) almacenar múltiples copias de información valiosa en soportes de almacenamiento separados para reducir aún más el riesgo de daños o pérdidas fortuitas de información;

g) considerar el registro de soportes de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;

h) habilitar los puertos de medios de almacenamiento extraíbles [por ejemplo, ranuras para tarjetas SD (SD Secure Digital) y puertos USB (Universal Serial Bus) sólo si existe una razón organizativa para su uso;

i) cuando sea necesario utilizar soportes de almacenamiento extraíbles, controlar la transferencia de información a dichos medios de almacenamiento;

j) la información puede ser vulnerable al acceso no autorizado, al uso indebido o a la corrupción durante el transporte físico, por ejemplo, al enviar medios de almacenamiento a través del servicio postal o por mensajería.

En este control, los soportes incluyen los documentos en papel. Al transferir soportes físicos, aplique las medidas de seguridad indicadas en el apartado 5.14.

Reutilización o eliminación segura

Deberían establecerse procedimientos para la reutilización o eliminación segura de los soportes de almacenamiento con el fin de minimizar el riesgo de filtración de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación segura de soportes de almacenamiento que contengan información confidencial deberían ser proporcionales a la sensibilidad de dicha información. Deberían tenerse en cuenta los siguientes elementos:

a) si es necesario reutilizar dentro de la organización soportes de almacenamiento que contengan información confidencial, eliminar los datos de forma segura o formatear el soporte de almacenamiento antes de reutilizarlo (véase 8.10);

b) eliminar de forma segura los soportes de almacenamiento que contengan información confidencial cuando ya no se necesiten (por ejemplo, destruyendo, triturando o borrando de forma segura el contenido);

c) disponer de procedimientos para identificar los dispositivos que pueden requerir una eliminación segura;

d) muchas organizaciones ofrecen servicios de recogida y eliminación de soportes de almacenamiento. Debería tenerse cuidado a la hora de seleccionar un proveedor externo adecuado que cuente con los controles y la experiencia adecuados;

e) registrar la eliminación de dispositivos sensibles para mantener una pista de auditoría;

f) al acumular soportes de almacenamiento para su eliminación, tener en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se convierta en sensible.

Debería realizarse una evaluación de riesgos de los dispositivos dañados que contengan datos sensibles para determinar si los dispositivos deberían destruirse físicamente en lugar de enviarlos a reparar o desecharlos (véase 7.14).

Información adicional

Cuando la información confidencial de los soportes de almacenamiento no está cifrada, debería considerarse la posibilidad de proteger físicamente los soportes de almacenamiento.

7.11 Instalaciones de suministro

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección

Control

Las instalaciones de procesamiento de información deberían estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

Propósito

Evitar la pérdida, el daño o compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a fallos e interrupciones de las instalaciones de suministro.

Orientación

Las organizaciones dependen del suministro de servicios esenciales (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para apoyar sus instalaciones de tratamiento de la información. Por lo tanto, la organización debería:

a) garantizar que los equipos de soporte a los servicios estén configurados, funcionen y se mantengan de acuerdo con las especificaciones del fabricante correspondiente;

b) garantizar que se evalúa periódicamente la capacidad del suministro para hacer frente al crecimiento empresarial y a las interacciones con otros servicios de apoyo;

c) garantizar que los equipos de soporte a los servicios se inspeccionan y prueban periódicamente para garantizar su correcto funcionamiento;

d) en caso necesario, activar alarmas para detectar averías en los servicios;

e) si es necesario, garantizar que los servicios esenciales dispongan de varias alimentaciones de suministro con diversos encaminamientos físicos;

f) garantizar que los equipos de soporte a los servicios estén en una red separada de las instalaciones de tratamiento de la información, si están conectadas a una red;

g) garantizar que los equipos de soporte a los servicios se conecten a Internet sólo cuando sea necesario y de forma segura.

Se debería proporcionar iluminación y comunicaciones de emergencia. Los interruptores y válvulas de emergencia para cortar la electricidad, el agua, el gas u otros servicios deberían ubicarse cerca de las salidas de emergencia o salas de equipos. Los datos de contacto de emergencia deberían registrarse y estar disponibles para el personal en caso de una interrupción.

Información adicional

Se puede obtener ¿redundancia? adicional para la conectividad de red mediante múltiples rutas de más de un proveedor de servicios.

7.12 Seguridad del cableado

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.

Propósito

Evitar la pérdida, daño, robo o compromiso de información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

Orientación

Se deberían considerar las siguientes directrices para la seguridad del cableado:

a) que las líneas eléctricas y de telecomunicaciones que llegan a las instalaciones de tratamiento de la información sean soterradas siempre que sea posible, o que se adopte medidas alternativas de protección, como un protector de cables en el suelo o postes; si los cables son subterráneos, protegerlos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia);

b) separar los cables de energía de los cables de comunicaciones para evitar interferencias;

c) para sistemas sensibles o críticos, otros controles a considerar incluyen:

   1) instalación de conductos blindados y cajas o salas cerradas y alarmas en los puntos de inspección y terminación;

   2) uso de blindaje electromagnético para proteger los cables;

   3) implantación de barreras técnicas e inspecciones físicas para detectar la conexión al cableado de dispositivos no autorizados;

   4) accesos controlados a los paneles de conexión y a las salas de cableado (por ejemplo, con llaves mecánicas o claves PINs);

   5) uso de cables de fibra óptica;

d) etiquetar los cables en cada extremo con suficientes indicaciones de origen y destino para permitir la identificación física y la inspección del cable.

Se debería buscar asesoramiento especializado sobre cómo gestionar los riesgos derivados de incidentes de cableado o mal funcionamiento.

Información adicional

A veces, el cableado eléctrico y de telecomunicaciones son recursos compartidos por más de una organización que ocupa locales comunes.

7.13 Mantenimiento de los equipos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_Activos	#Protección #Resiliencia

Control

Los equipos deberían recibir un mantenimiento correcto que asegure la disponibilidad, integridad y confidencialidad de la información.

Propósito

Prevenir la pérdida, daño, robo o puesta en peligro de la información y otros activos asociados, así como la interrupción de las operaciones de la organización causada por la falta de mantenimiento.

Orientación

Se deberían considerar las siguientes directrices para el mantenimiento de los equipos:

a) mantener los equipos de acuerdo con la frecuencia y las especificaciones de servicio recomendadas por el proveedor;

b) implementar y supervisar un programa de mantenimiento por parte de la organización;

c) sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y el servicio de los equipos;

d) mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo;

e) implementar controles apropiados cuando los equipos estén programados para mantenimiento, teniendo en cuenta si este mantenimiento lo realiza personal *in situ* o externo a la organización; sometiendo al personal de mantenimiento a un acuerdo de confidencialidad adecuado;

f) supervisar al personal de mantenimiento cuando realice tareas de mantenimiento *in situ*;

g) autorizar y controlar el acceso para el mantenimiento realizado en remoto;

h) aplicar medidas de seguridad para los activos fuera de los locales (véase 7.9) si los equipos que contienen información se sacan de los locales para su mantenimiento;

i) cumplir todos los requisitos de mantenimiento impuestos por los seguros;

j) antes de volver a poner en funcionamiento el equipo tras el mantenimiento, inspeccionarlo para asegurarse de que no ha sido manipulado y funciona correctamente;

k) aplicar medidas para la eliminación segura o la reutilización de los equipos (véase 7.14) si se determina que los equipos que tienen que eliminarse.

Información adicional

El equipamiento incluye componentes técnicos de instalaciones de tratamiento de la información, sistemas de alimentación ininterrumpida (SAI) y baterías, generadores de energía, alternadores y convertidores de energía, sistemas de detección de intrusión física y alarmas, detectores de humo, extintores, aire acondicionado y ascensores

7.14 Eliminación o reutilización segura de los equipos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_Física #Gestión_de_activos	#Protección

Control

Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y *software* bajo licencia han sido eliminados o sobrescritos de manera segura, antes de deshacerse de ellos o reutilizarlos.

Propósito

Evitar fugas de información de los equipos que se van a eliminar o reutilizar.

Orientación

Debería comprobarse si los equipos contienen medios de almacenamiento o no antes de su eliminación o reutilización.

Los soportes que contengan información confidencial o con derechos de autor deberían ser destruidos físicamente o bien la información debería ser destruida, borrada o sobrescrita mediante técnicas que hagan imposible la recuperación de la información original, en lugar de utilizar un borrado o un formateado normal. Véase el apartado 7.10 para obtener orientaciones detalladas sobre la eliminación segura de soportes de almacenamiento y el apartado 8.10 para obtener orientaciones sobre la eliminación de información.

Las etiquetas y marcas que identifiquen a la organización o indiquen la clasificación, el propietario, el sistema o la red, deberían retirarse antes de su eliminación, incluida su reventa o su donación a organizaciones benéficas.

La organización debería considerar la eliminación de los controles de seguridad, como los controles de acceso o los equipos de vigilancia, al final del contrato de arrendamiento o cuando se traslade fuera de las instalaciones. Esto depende de factores como:

a) el contrato de arrendamiento para devolver las instalaciones a su estado original;

b) minimizar el riesgo de dejar sistemas con información sensible para el siguiente arrendatario (por ejemplo, listas de acceso de usuarios, archivos de vídeo o imagen);

c) la posibilidad de reutilizar los controles en la siguiente instalación.

Información adicional

Los equipos dañados que contienen soportes de almacenamiento pueden requerir una evaluación de riesgos para determinar si los artículos deberían destruirse físicamente en lugar de enviarlos a reparar o desecharlos. La información puede verse comprometida por una eliminación o reutilización descuidada de los equipos.

Además del borrado seguro del disco, el cifrado de todo el disco reduce el riesgo de revelación de información confidencial cuando el equipo se desecha o se reubica, siempre que:

a) el proceso de cifrado sea suficientemente fuerte y cubra el disco completamente (incluyendo el espacio libre, archivos temporales de intercambio de memoria, etc.);

b) las claves criptográficas son lo suficientemente largas como para resistir ataques de fuerza bruta;

c) las claves criptográficas se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para consejos adicionales sobre cifrado, véase el apartado 8.24.

Las técnicas para sobrescribir de forma segura los soportes de almacenamiento difieren en función de la tecnología del soporte y del nivel de clasificación de la información en el soporte. Las herramientas de sobreescritura deberían ser revisadas para asegurarse de que son aplicables a la tecnología del soporte de almacenamiento.

Consulte la Norma ISO/IEC 27040 para obtener información detallada sobre los métodos de saneamiento de los soportes de almacenamiento.

8 Controles tecnológicos

8.1 Dispositivos finales de usuario

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	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 finales de usuario debería protegerse.

Propósito

Proteger la información contra los riesgos introducidos por el uso de dispositivos finales de usuario.

Orientación

General

La organización debería establecer una directiva específica sobre la configuración y el manejo seguros de los dispositivos finales de usuario. La política específica debería comunicarse a todo el personal relevante y considerar lo siguiente:

a) el tipo de información y el nivel de clasificación que los dispositivos finales de usuario pueden manejar, procesar, almacenar o soportar;

b) registro de dispositivos finales de usuario;

c) requisitos de protección física;

d) restricción de la instalación de *software* (por ejemplo, controlada remotamente por administradores del sistema);

e) requisitos para el *software* del dispositivo final del usuario (incluidas las versiones de *software*) y para aplicar actualizaciones (por ejemplo, actualización automática activa);

f) normas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones (por ejemplo, exigiendo el uso de un cortafuegos personal);

g) controles de acceso;

h) cifrado del dispositivo de almacenamiento;

i) protección contra código malicioso;

j) desactivación, supresión o bloqueo a distancia;

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 los puertos físicos (por ejemplo, puertos USB);

o) el uso de capacidades de partición, si es compatible con el dispositivo 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 dispositivos finales de usuario, pero no se almacena en dichos dispositivos. En tales casos, se podría requerir salvaguardas 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 ser conscientes de los requisitos y procedimientos de seguridad para proteger los dispositivos finales de los usuarios, así como de sus responsabilidades para implementar dichas medidas de seguridad. Se debería aconsejar a los usuarios:

a) cerrar las sesiones activas y terminar los servicios cuando ya no sean necesarios;

b) proteger los dispositivos finales de los usuarios contra el uso no autorizado mediante un control físico (por ejemplo, cerradura con llave o cerraduras especiales) y un control lógico (por ejemplo, acceso mediante contraseña) cuando no estén en uso; no dejar desatendidos los dispositivos que transporten información empresarial importante, sensible o crítica;

c) utilizar dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas (por ejemplo, evitar leer información confidencial si las personas pueden leer desde atrás, utilizar filtros de privacidad en la pantalla);

d) proteger físicamente los dispositivos finales de los usuarios contra robos (por ejemplo, en coches y otros medios de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

Se debería establecer un procedimiento específico que tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales (incluyendo el seguro) y otros requisitos de seguridad de la organización para los casos de robo o pérdida de dispositivos finales de usuario.

Uso de dispositivos personales

Cuando la organización permite el uso de dispositivos personales (a veces conocidos como BYOD), además de la orientación dada en este control, se debería considerar lo siguiente:

a) separación del uso personal y profesional de los dispositivos, incluyendo el uso de *software* para respaldar dicha separación y proteger los datos profesionales en un dispositivo privado;

b) proporcionar acceso a la información profesional solo después de que los usuarios hayan reconocido sus obligaciones (protección física, actualización de *software*, etc.), renunciar a la propiedad de los datos profesionales, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no esté autorizado a usar el servicio. En tales casos, se debería considerar la legislación de protección de datos personales;

c) políticas y procedimientos específicos para evitar conflictos relativos a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

d) acceso a equipos de propiedad privada (para verificar la seguridad del dispositivo o durante una investigación), que puede ser impedido por la legislación;

e) acuerdos de licencia de *software* que sean tales que las organizaciones puedan ser responsables de la concesión de licencias de *software* en dispositivos finales de usuario, siendo el dispositivo propiedad privada del empleado o de usuarios externos.

Conexiones inalámbricas

La organización debería establecer procedimientos para:

a) la configuración de conexiones inalámbricas en dispositivos (por ejemplo, desactivando los protocolos vulnerables);

b) utilizar conexiones inalámbricas o por cable con el ancho de banda adecuado de acuerdo con las políticas específicas pertinentes (por ejemplo, porque se necesitan hacer copias de seguridad o actualizaciones de *software*).

Información adicional

Los controles para proteger la información en los dispositivos finales de usuario dependen de si se utiliza sólo dentro de las instalaciones y conexiones de red seguras de la organización, o si está expuesto a mayores amenazas físicas y de red fuera de la organización.

Las conexiones inalámbricas para dispositivos finales de usuario son similares a otros tipos de conexiones de red, pero presentan diferencias importantes que deberían tenerse en cuenta a la hora de identificar los controles. En particular, la copia de seguridad de la información almacenada en los dispositivos finales de usuario puede fallar a veces debido a un ancho de banda de red limitado o porque los dispositivos finales de usuario no están conectados en los momentos en que están programadas 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 Gestión de privilegios de acceso

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_de_acceso	#Protección

Control

La asignación y el uso de derechos de acceso con privilegios debería ser restringido y controlado.

Propósito

Garantizar que sólo los usuarios, componentes de *software* y servicios autorizados dispongan de derechos de acceso privilegiados.

Orientación

La asignación de derechos de acceso privilegiados debería controlarse mediante un proceso de autorización de conformidad con la política específica correspondiente sobre control de acceso (véase 5.15). Se debería considerar lo siguiente:

a) identificar a los usuarios que necesitan derechos de acceso privilegiados para cada sistema o proceso (por ejemplo, sistemas operativos, sistemas de gestión de bases de datos y aplicaciones);

b) asignar derechos de acceso privilegiado a los usuarios según sea necesario y en función de cada evento, de acuerdo con la política específica sobre control de acceso (véase 5.15) (es decir, sólo a las personas con la competencia necesaria para llevar a cabo actividades que requieran acceso privilegiado y sobre la base de los requisitos mínimos para sus roles funcionales);

c) mantener un proceso de autorización (es decir, determinar quién puede aprobar derechos de acceso privilegiado, o no conceder derechos de acceso privilegiado hasta que el proceso de autorización se haya completado) y un registro de todos los privilegios asignados;

d) definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado;

e) tomar medidas para garantizar que los usuarios son conscientes de sus derechos de acceso privilegiado y de cuándo se encuentran en modo de acceso privilegiado. Entre las posibles medidas se incluyen el uso de identidades de usuario específicas, la configuración de la interfaz de usuario o incluso equipos específicos;

f) los requisitos de autenticación para los derechos de acceso privilegiados pueden ser superiores a los requisitos para los derechos de acceso normales. Puede ser necesaria una nueva autenticación o un paso de autenticación antes de trabajar con derechos de acceso privilegiados;

g) revisar periódicamente, y después de cualquier cambio organizativo, a los usuarios que trabajan con derechos de acceso privilegiados para comprobar si sus funciones, roles, responsabilidades y competencias siguen habilitadas para trabajar con derechos de acceso privilegiados (véase 5.18);

h) establecer reglas específicas para evitar el uso de identidades genéricas de usuario de administración (como "root"), en función de las capacidades de configuración de los sistemas. Gestionar y proteger la información de autenticación de dichas identidades (véase 5.17);

i) conceder acceso privilegiado temporal sólo durante el tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de conceder permanentemente derechos de acceso privilegiado. Esto suele denominarse procedimiento "break glass" ("Romper el cristal" un medio rápido para extender los derechos de acceso de una persona en casos excepcionales y solo debería usarse cuando los procesos normales son insuficientes), y a menudo se automatiza mediante tecnologías de gestión de acceso privilegiado;

j) registrar todos los accesos privilegiados a los sistemas con fines de auditoría;

k) no compartir o vincular identidades con derechos de acceso privilegiado a múltiples personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiado específicos. Las identidades pueden agruparse (por ejemplo, definiendo un grupo de administradores) para simplificar la gestión de los derechos de acceso privilegiado;

l) utilizar únicamente identidades con derechos de acceso privilegiados para llevar a cabo tareas administrativas y no para tareas generales cotidianas [es decir, consultar el correo electrónico, acceder a la web (los usuarios deberían tener una identidad de red normal separada para estas actividades)].

Información adicional

Los derechos de acceso privilegiados son derechos de acceso proporcionados a una identidad, un rol o un proceso que permite la realización de actividades que los usuarios o procesos típicos no pueden realizar. Las funciones de administrador del sistema suelen requerir derechos de acceso privilegiados.

El uso inadecuado de los privilegios de administrador del sistema (cualquier característica o facilidad de un sistema de información que permita al usuario anular los controles del sistema o de la aplicación) es uno de los principales factores que contribuyen a los fallos o violaciones de los sistemas.

Para más información sobre la gestión de accesos y la gestión segura del acceso a la información y a los recursos de las tecnologías de la información y la comunicación, consulte la Norma ISO/IEC 29146.

8.3 Restricción del acceso a la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_de_acceso	#Protección

Control

Se debería restringir el acceso a la información y otros activos relacionados, de acuerdo con las políticas específicas de control de acceso definidas.

Propósito

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

Orientación

El acceso a la información y otros activos asociados debería restringirse de acuerdo con las políticas específicas establecidas. Para apoyar los requisitos de restricción de acceso debería considerarse lo siguiente:

a) no permitir el acceso a información sensible por parte de identidades de usuario desconocidas o anónimas. El acceso público o anónimo solo debería concederse a las ubicaciones de almacenamiento que no contengan ninguna 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 concreto;

d) controlar qué identidades o grupos de identidades tienen determinados accesos, como accesos de 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, se deberían considerar técnicas y procesos de gestión de acceso dinámico para proteger la información sensible que tiene un alto valor para la organización cuando la organización:

a) necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera;

b) quiere compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a ella;

c) quiere gestionar dinámicamente, en tiempo real, el uso y la distribución de dicha información;

d) quiere proteger dicha información contra cambios, copia y distribución no autorizados (incluida la impresión);

e) quiere controlar el uso de la información;

f) quiere registrar cualquier cambio en dicha información que tenga lugar en caso de que se requiera una investigación futura.

Las técnicas de gestión de acceso dinámico deberían proteger la información a lo largo de su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) establecer normas sobre la gestión del acceso dinámico basadas en casos de uso específicos teniendo en cuenta:

    1) conceder permisos de acceso en función de la identidad, del dispositivo, de la ubicación o de la aplicación;

    2) aprovechar el esquema de clasificación para determinar qué información debería protegerse con técnicas de gestión dinámica de acceso;

b) establecer procesos operacionales, de supervisión y de elaboración de informes, así como infraestructura técnica de apoyo.

Los sistemas de gestión de acceso dinámico deberían proteger la información:

a) exigiendo autenticación, credenciales adecuadas o un certificado para acceder a la información;

b) restringiendo el acceso, por ejemplo, a un plazo determinado (por ejemplo, después de una fecha determinada o hasta una fecha determinada);

c) utilizando el cifrado para proteger la información;

d) definiendo los permisos de impresión de la información;

e) registrando quién accede a la información y cómo se utiliza la información;

f) emitiendo alertas si se detectan intentos de uso indebido de la información.

Información adicional

Las técnicas de gestión de acceso dinámico y otras tecnologías dinámicas de protección de la información pueden respaldar la protección de la información incluso cuando los datos se comparten más allá de la organización de origen, donde no se pueden aplicar los controles de acceso tradicionales. Se puede aplicar a documentos, correos electrónicos u otros archivos que contengan información para limitar quién puede acceder al contenido y de qué manera. Puede ser a 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 clásica del acceso [por ejemplo, utilizando listas de control de acceso (ACL)], pero pueden añadir más factores de condicionalidad, evaluación en tiempo real, reducción de datos justo a tiempo y otras mejoras que pueden ser útiles para la información más sensible. Así se proporciona una forma de controlar el acceso fuera del entorno de la organización. La respuesta a incidentes puede apoyarse en técnicas de gestión de acceso dinámico, ya que los permisos pueden modificarse o revocarse en cualquier momento.

Se proporciona información adicional sobre un marco para la gestión del acceso en la Norma ISO/IEC 29146.

8.4 Acceso al código fuente

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_de_acceso #Seguridad_de_las_aplicaciones #Configuración_segura	#Protección

Control

Se debería gestionar adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de *software*.

Propósito

Impedir la introducción de funcionalidades no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

Orientación

El acceso al código fuente y los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y herramientas de desarrollo (por ejemplo, compiladores, generadores de código, 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 de 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 abierto o componentes de código de terceros dentro de una organización, se puede proporcionar ampliamente el acceso de lectura a dichos repositorios de código externo. Sin embargo, el acceso de escritura aún debería estar restringido.

Se deberían considerar las siguientes directrices para controlar el acceso al código fuente de programas a fin de reducir el potencial de corrupción de los programas informáticos:

a) gestionar el acceso al código fuente de los programas y a las bibliotecas de código fuente de acuerdo con los procedimientos establecidos;

b) conceder acceso de lectura y escritura al código fuente en función de las necesidades de la empresa y gestionado para hacer frente a los riesgos de alteración o uso indebido y de acuerdo con los procedimientos establecidos;

c) la actualización del código fuente y los elementos asociados y la concesión de acceso al código fuente de conformidad con los procedimientos de control de cambios (véase 8.32), y sólo llevarse a cabo tras haber recibido la autorización correspondiente;

d) no conceder a los desarrolladores acceso directo al repositorio de código fuente, sino a través de herramientas de desarrollo que controlan las actividades y autorizaciones sobre el código fuente;

e) mantener los listados de programas en un entorno seguro, donde el acceso de lectura y escritura debería gestionarse y asignarse adecuadamente;

f) mantener un registro de auditoría de todos los accesos y de todos los cambios en el código fuente.

Si se pretende publicar el código fuente del programa, deberían considerarse controles adicionales que garanticen su integridad (por ejemplo, firma digital).

Información adicional

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	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_accesos	#Protección

Control

Las tecnologías y procedimientos de autenticación segura deberían implementarse en función de las restricciones de acceso a la información y la política específica sobre control de acceso.

Propósito

Garantizar que un usuario o una entidad esté autenticado de forma segura cuando se le concede acceso a los sistemas, aplicaciones y servicios.

Orientación

Debería elegirse una técnica de autenticación adecuada para justificar la identidad reivindicada de un usuario, *software*, mensajes y otras entidades.

La solidez de la autenticación debería ser adecuada de acuerdo con la clasificación de la información a la que se va a acceder. Cuando se requiera una autenticación y verificación de identidad sólidas, deberían utilizarse métodos de autenticación alternativos a las contraseñas, tales como certificados digitales, tarjetas inteligentes, dispositivos o medios biométricos.

La información de autenticación debería ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información críticos (conocida también como autenticación multifactorial). El uso de una combinación de factores múltiples de autenticación, algo que sabes, algo que tienes y que eres, reduce las posibilidades de accesos no autorizados. La autenticación multifactorial 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, a través de un dispositivo inusual o en un momento inusual.

La información utilizada para la 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 anticiparse a estos problemas y estar preparados, 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 teniendo en cuenta lo siguiente:

a) no mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito, para evitar proporcionar a un usuario no autorizado cualquier tipo de información innecesaria;

b) mostrar un aviso general advirtiendo que el acceso al sistema, a la aplicación o al servicio solo debería ser efectuado por aquellos usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión, que podrían brindar información importante a usuarios no autorizados (por ejemplo, si surge un error, el sistema no debería indicar qué parte de los datos introducidos son correctos o incorrectos);

d) validar la información de inicio de sesión sólo cuando estén completos todos los datos de entrada requeridos;

e) proteger el nombre de usuario y contraseña en el inicio de sesión, contra ataques de fuerza bruta [por ejemplo, utilizando una prueba de Turing pública completamente automatizada para diferenciar entre computadoras y humanos (CAPTCHA), requiriendo el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o bloqueando al usuario después de un número máximo de errores al intentar iniciar sesión];

f) registrar intentos fallidos y exitosos;

g) generar un evento de seguridad si se detecta un posible intento de violación o bien una violación, exitosa 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 ha alcanzado un determinado número de contraseñas incorrectas introducidas, al intentar iniciar sesión);

h) enseñar o enviar la siguiente información mediante un canal de comunicación distinto, al iniciar correctamente la sesión:

   1) fecha y hora del último inicio de sesión exitoso;

   2) detalles de cualquier intento de inicio de sesión fallido desde el último inicio de sesión exitoso;

i) no enseñar una contraseña en texto legible cuando se escribe la misma en el cuadro de inicio de sesión; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario (por ejemplo, por razones de accesibilidad o para evitar el bloqueo de usuarios debido a la reiteración de errores);

j) no transmitir contraseñas en texto legible, a través de una red, para evitar que sean capturadas por un "sniffer" de red;

k) finalizar las sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo, tales como áreas públicas o externas fuera del alcance de la administración de seguridad de la organización o en dispositivos finales de usuario;

l) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo y reducir la ventana de oportunidad para los accesos no autorizados.

Información adicional

Puede encontrar información adicional sobre garantía de autenticación de entidades en la Norma ISO/IEC 29115.

8.6 Gestión de capacidades

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Continuidad	#Gobernanza_y_Ecosistema #Protección

Control

Se debería supervisar y ajustar la utilización de los recursos en consonancia con los requisitos de capacidad actuales y esperados.

Propósito

Asegurar la capacidad requerida, tanto de las instalaciones de tratamiento de la información, como de los recursos humanos, oficinas y otras instalaciones.

Orientación

Deberían identificarse las necesidades de capacidad para las instalaciones de tratamiento de la información, los recursos humanos, las oficinas y otras instalaciones, teniendo en cuenta la importancia comercial de los sistemas y procesos de que se trate.

Debería supervisarse y adaptarse el sistema para garantizar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas.

La organización debería realizar pruebas de estrés de los sistemas y servicios para confirmar que el sistema dispone de la capacidad suficiente para cumplir con los requisitos de rendimiento máximo.

Se deberían establecer controles de detección para descubrir problemas a tiempo.

Las proyecciones a futuro de las necesidades de capacidad, deberían tener en consideración las nuevas necesidades de negocio y de sistemas y las tendencias actuales y proyectadas de la capacidad de procesamiento de la información de la organización.

Se debería prestar especial atención a cualquier recurso que suponga una adquisición a largo plazo o bien suponga un coste alto para la organización. Por lo tanto, los gerentes, propietarios de servicios o productos deberían supervisar la utilización de los recursos clave del sistema.

Los gerentes deberían usar la información sobre capacidad para identificar y evitar posibles limitaciones de recursos y de dependencia del personal clave que pueden presentar una amenaza para la seguridad o los servicios del sistema y planificar las acciones apropiadas.

Se puede lograr proporcionar la capacidad suficiente aumentando la capacidad o reduciendo la demanda. Debería considerarse lo siguiente con el fin de aumentar la capacidad:

a) contratar nuevo personal;

b) obtener nuevas instalaciones o espacio;

c) adquirir sistemas de procesamiento, memoria y almacenamiento más potentes;

d) hacer uso de la computación en la nube, que cuenta con características inherentes que abordan directamente los problemas de capacidad. La computación en la nube dispone de una elasticidad y escalabilidad que permiten una rápida expansión bajo demanda y la reducción de los recursos disponibles para determinadas aplicaciones y servicios.

Debería considerarse lo siguiente para reducir la demanda de recursos de la organización:

a) borrar información obsoleta (liberar espacio en disco);

b) eliminar registros impresos que hayan cumplido con su período de retención (liberar espacio en las estanterías);

c) retirar aplicaciones, sistemas, bases de datos o entornos;

d) optimizar procesos y programaciones por lotes;

e) optimizar el código de aplicación o las consultas de base de datos;

f) denegar o restringir el ancho de banda para los servicios que consumen recursos si estos no son críticos (por ejemplo, transmisión de vídeo).

Se debería considerar un plan documentado de gestión de la capacidad para los sistemas de misión crítica.

Información adicional

Para obtener más detalles sobre la elasticidad y escalabilidad de la computación en nube, consulte la Especificación Técnica ISO/IEC TS 23167.

8.7 Controles contra el código malicioso

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_del_Sistema_y_de_la_red #Protección_de_la_información	#Protección #Defensa

Control

Se debería implementar una protección contra el código malicioso, respaldada por una concienciación adecuada al usuario.

Propósito

Garantizar que la información y otros activos asociados estén protegidos contra el código malicioso.

Orientación

La protección contra el código malicioso debería basarse en *software* de detección y reparación de código dañino, concienciación sobre la seguridad de la información, acceso adecuado al sistema y controles de gestión de cambios. El uso de *software* de detección y reparación de código malicioso por sí solo no suele ser adecuado. Deberían considerar las siguientes orientaciones:

a) implementar normas y controles que impidan o detecten el uso de programas informáticos no autorizados [por ejemplo, listas de aplicaciones permitidas (es decir, utilizando una lista que proporcione aplicaciones permitidas)] (véanse 8.19 y 8.32);

b) implementar controles que impidan 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 el código malicioso [por ejemplo, a través de la gestión de vulnerabilidades técnicas (véanse 8.8 y 8.19)];

d) llevar a cabo una validación automatizada periódica del *software* y el contenido de los datos de los sistemas, especialmente para los sistemas que soportan procesos comerciales críticos; investigar la presencia de archivos no aprobados o modificaciones no autorizadas;

e) establecer medidas de protección contra los riesgos asociados con la obtención de archivos y *software*, ya sea de redes externas o por cualquier otro medio;

f) instalar y actualizar regularmente el *software* de detección y reparación de código dañino para escanear computadoras y medios de almacenamiento electrónico. Llevar a cabo exploraciones regulares que incluyen:

   1) escanear cualquier dato recibido a través de redes o a través de cualquier forma de almacenamiento electrónico, en busca de código malicioso antes de su uso;

   2) escanear correos electrónicos y sus archivos adjuntos y mensajería instantánea y descargas en busca de código malicioso antes de su uso. Llevar a cabo este escaneo en diferentes lugares (por ejemplo, en los servidores de correo electrónico, computadoras de escritorio) y al ingresar a la red de la organización;

   3) analizar páginas web en busca de código malicioso cuando se accede a ellas.

g) determinar la ubicación y configuración de las herramientas de detección y reparación de código malicioso en función de los resultados de la evaluación de riesgos y considerar:

   1) defensa en profundidad, donde serían más eficaces. Por ejemplo, esto puede conducir a la detección de código malicioso en una puerta de enlace de red (en varios protocolos de aplicación como correo electrónico, transferencia de archivos y web), así como en dispositivos y servidores de punto final de usuario;

   2) las técnicas evasivas utilizadas por los atacantes (por ejemplo, el uso de archivos cifrados) para distribuir código malicioso o el uso de protocolos de cifrado para transmitir código malicioso.

h) protegerse contra la introducción de código malicioso durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra el código malicioso.

i) implementar un proceso para autorizar la desactivación temporal o permanente de algunas o todas las medidas contra el código malicioso, incluyendo a las autoridades que aprueban las excepciones, la justificación documentada y la fecha de revisión. Esto puede llegar a ser necesario cuando la protección contra el código malicioso causa interrupciones en las operaciones normales;

j) preparar planes de continuidad adecuados para recuperarse de ataques de programas maliciosos, incluyendo copias de seguridad todos los datos y programas informáticos necesarios (incluidas las copias de seguridad en línea y fuera de línea) y las medidas de recuperación (véase 8.13);

k) aislar aquellos entornos en los que pueden producirse consecuencias catastróficas.

l) definir procedimientos y responsabilidades para tratar la protección contra programas maliciosos en los sistemas, incluida la formación sobre su uso, la notificación y la recuperación en caso de ataques de programas maliciosos;

m) concienciar o formar (véase 6.3) a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, envío o instalación de correos electrónicos, archivos o aplicaciones infectados con código malicioso [la información recogida en n) y o) puede utilizarse para garantizar que la concienciación y la formación se mantengan actualizadas];

n) aplicar procedimientos para recabar periódicamente información sobre nuevos programas maliciosos, como suscribirse a listas de correo o consultar sitios web relevantes;

o) verificar que la información relativa a los programas maliciosos, como los boletines de alerta, proceden de fuentes cualificadas y reputadas (por ejemplo, sitios de Internet fiables o proveedores de programas informáticos de detección de programas maliciosos) y es exacta e informativa.

Información adicional

En algunos sistemas (por ejemplo, algunos sistemas de control industrial) no siempre es posible instalar *software* que proteja contra el código malicioso. Algunos tipos de código malicioso infectan los sistemas operativos y el firmware de los ordenadores de tal manera que, los controles comunes de código malicioso, no pueden limpiar el sistema y es necesario volver a crear una imagen completa del *software* del sistema operativo y, a veces, del firmware del ordenador para volver a un estado seguro.

8.8 Gestión de vulnerabilidades técnicas

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión_de_amenazas_y_de_vulnerabilidades	#Gobernanza_y_Ecosistema #Protección #Defensa

Control

Se debería obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas.

Propósito

Evitar la explotación de vulnerabilidades técnicas.

Orientación

Identificar las vulnerabilidades técnicas

La organización debería disponer de un inventario preciso de activos (véanse 5.9 a 5.14) como requisito previo para una gestión eficaz de la vulnerabilidad técnica; el inventario debería incluir al proveedor del *software*, el nombre del *software*, los números de versión, el estado actual de despliegue (por ejemplo, qué *software* está instalado en qué sistemas) y la persona o personas de la organización responsables del *software*.

Para identificar las vulnerabilidades técnicas, la organización debería considerar:

a) definir y establecer las funciones y responsabilidades asociadas a la gestión técnica de la vulnerabilidad, incluida la supervisión de la vulnerabilidad, la evaluación del riesgo de vulnerabilidad, la actualización, el seguimiento de los activos y cualquier responsabilidad de coordinación necesaria;

b) identificar, para los programas informáticos y otras tecnologías (basándose en la lista del inventario de activos, véase 5.9), los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y mantener el conocimiento sobre ellas. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles;

c) exigir a los proveedores de sistemas de información (incluidos sus componentes) que garanticen la notificación, el tratamiento y la divulgación de las vulnerabilidades, incluyendo estos requisitos en los respectivos contratos (véase 5.20);

d) utilizar herramientas de exploración de vulnerabilidades, adecuadas a las tecnologías actuales, para identificar vulnerabilidades y verificar si el parcheado de vulnerabilidades se ha realizado correctamente;

e) realizar pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles, por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades. Proceder con cautela, ya que estas actividades pueden comprometer la seguridad del sistema;

f) rastrear el uso de bibliotecas y código fuente de terceros en busca de vulnerabilidades. Esto debería incluirse en la codificación segura (véase 8.28).

La organización debería desarrollar procedimientos y facultades para:

a) detectar la existencia de vulnerabilidades en sus productos y servicios, incluyendo cualquier componente externo utilizado en los mismos;

b) recibir informes sobre vulnerabilidades de fuentes internas o externas.

La organización debería proporcionar un punto de contacto público como parte de una política específica sobre divulgación de vulnerabilidades para que los investigadores y otras personas puedan informar de los problemas. La organización debería establecer procedimientos de notificación de vulnerabilidades, formularios de notificación en línea y hacer uso de los foros adecuados de inteligencia de amenazas o de intercambio de información. La organización también debería considerar programas de recompensas en los que se ofrezcan recompensas como incentivo para ayudar a las organizaciones a identificar vulnerabilidades con el fin de remediarlas adecuadamente. La organización también debería compartir información con los organismos competentes del sector u otras partes interesadas.

Evaluación de vulnerabilidades técnicas

Deberían tenerse en cuenta las siguientes orientaciones para evaluar las vulnerabilidades técnicas identificadas:

a) analizar y verificar los informes para determinar qué tipo de actividad de respuesta y reparación es necesaria;

b) una vez identificada una posible vulnerabilidad técnica, determinar los riesgos asociados y las medidas que tienen que adoptarse. Dichas acciones pueden implicar la actualización de los sistemas vulnerables o la aplicación de otros controles.

Adoptar las medidas adecuadas para hacer frente a las vulnerabilidades técnicas

Debería implementarse un proceso de gestión de actualizaciones de *software* para garantizar que se instalan los parches aprobados y las actualizaciones de aplicaciones más recientes para todo el *software* autorizado. Si es necesario realizar cambios, se debería conservar el *software* original y aplicar los cambios a una copia designada. Todos los cambios deberían probarse y documentarse por completo, de modo que puedan volver a aplicarse, en caso necesario, a futuras actualizaciones de *software*. Si es necesario, las modificaciones deberían ser probadas y validadas por un organismo de evaluación independiente.

Deberían tenerse en cuenta las siguientes orientaciones para hacer frente a las vulnerabilidades técnicas:

a) tomar medidas adecuadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un calendario para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

b) en función de la urgencia con la que deba abordarse una vulnerabilidad técnica, se llevará a cabo la acción según los controles relacionados con la gestión del cambio (véase 8.32) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (véase 5.26);

c) utilizar únicamente actualizaciones de fuentes legítimas (que pueden ser internas o externas a la organización);

d) probar y evaluar las actualizaciones antes de que se instalen para garantizar que sean eficaces y no produzcan efectos secundarios que no puedan tolerarse [es decir, si hay una actualización disponible, evaluar los riesgos asociados con la instalación de la actualización (los riesgos planteados por la vulnerabilidad deberían compararse con el riesgo de instalar la actualización)]; probar y evaluar las actualizaciones antes de instalarlas para asegurarse de que son eficaces y no provocan efectos secundarios que no puedan tolerarse [es decir, si hay una actualización disponible, evaluar los riesgos asociados a 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) realizar pruebas para confirmar si la reparación o mitigación es efectiva;

h) proporcionar mecanismos para verificar la autenticidad de la reparación;

i) si no hay ninguna actualización disponible o la actualización no se puede instalar, hay que tener en consideración otros controles, como:

   1) aplicar cualquier solución sugerida por el proveedor de *software* o bien por otras fuentes relevantes;

   2) desactivar servicios o capacidades relacionadas con la vulnerabilidad.

3) adaptar o añadir controles de acceso (por ejemplo, cortafuegos) en las fronteras de la red (véanse 8.20 a 8.22);

4) proteger los sistemas, dispositivos o aplicaciones vulnerables de ataques mediante la implementación de filtros de tráfico adecuados (a veces llamados parches virtuales);

5) aumentar la supervisión para detectar ataques reales;

6) realizar concienciaciones sobre las vulnerabilidades.

Respecto del *software* adquirido, si los proveedores publican regularmente información sobre las actualizaciones de seguridad para su *software* y proporcionan la posibilidad de instalar dichas actualizaciones de forma automatizada para instalar dichas actualizaciones automáticamente, la organización debería decidir si usar la actualización automática o no.

Otras consideraciones

Se debería mantener un registro de auditoria para todos los pasos dados en la gestión de vulnerabilidades técnicas.

El proceso de gestión de las vulnerabilidades técnicas debería supervisarse y evaluarse periódicamente para garantizar su eficacia y eficiencia.

Un proceso eficaz de gestión de vulnerabilidades técnicas debería alinearse con las actividades de gestión de incidentes, para comunicar datos sobre las vulnerabilidades a la función de respuesta a incidentes con el fin de proporcionar aquellos procedimientos técnicos que se llevarán a cabo en caso de que ocurriera un incidente.

Cuando la organización utilice un servicio en la nube suministrado por un proveedor de servicios en la nube de terceros, dicho proveedor debería garantizar la gestión de las vulnerabilidades técnicas de los recursos de los servicios en la nube. La responsabilidad del proveedor de servicios en la nube respecto de la gestión de las vulnerabilidades técnicas debería formar parte del clausulado del acuerdo de servicio, incluyendo procesos para informar sobre las acciones del proveedor de servicios en la nube, relacionados con las vulnerabilidades técnicas (véase 5.23). Para determinados servicios en la nube, existen responsabilidades específicas, tanto para el proveedor de servicios como para el cliente. Por ejemplo, el cliente del servicio en la nube es responsable de la gestión de vulnerabilidades de sus propios activos, empleados para la utilización de los servicios en la nube.

Información adicional

La gestión de vulnerabilidades técnicas puede considerarse una subfunción de la gestión del cambio y, como tal, puede aprovechar los procesos y procedimientos para la gestión del cambio (véase 8.32).

Existe la posibilidad de que una actualización no aborde el problema adecuadamente y tenga efectos secundarios negativos. Además, en algunos casos, podría resultar difícil desinstalar una actualización que ya ha sido instalada.

Si no es posible realizar pruebas adecuadas de las actualizaciones (por ejemplo, debido a los costes o la falta de recursos), se puede considerar retrasar la instalación de la actualización, para evaluar los riesgos asociados sobre la base de la experiencia informada por otros usuarios. El uso de la Norma ISO/IEC 27031 puede ser beneficioso.

Cuando se producen actualizaciones de *software* o parches, la organización puede considerar proporcionar un proceso de actualización automatizado en el que estas actualizaciones se instalen en los sistemas o productos afectados, sin necesidad de la intervención por parte del cliente o del usuario. Si se ofrece un proceso de actualización automatizado, se le puede permitir al cliente o usuario la posibilidad de 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 automatizada es mantener el control sobre cuándo se realiza la actualización. Por ejemplo, un *software* utilizado para una determinada operación empresarial no se puede actualizar hasta que dicha operación se haya completado.

Una debilidad relacionada con el escaneo de vulnerabilidades es que, posiblemente, no tenga en cuenta, completamente, la profundidad de la defensa: dos contramedidas que siempre se invocan en secuencia pueden tener vulnerabilidades que están enmascaradas por fortalezas en la otra. Si bien la contramedida compuesta no es vulnerable, un escáner de vulnerabilidades puede informar que ambas medidas son vulnerables. Por lo tanto, la organización debería tener cuidado al revisar y actuar sobre los informes de vulnerabilidad.

Muchas organizaciones suministran *software*, sistemas, productos y servicios no solo dentro de la organización, sino también a partes interesadas, tales 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 correcciones y divulgar información sobre vulnerabilidades a los usuarios (normalmente a través de un aviso público) y proporcionar la información adecuada para los servicios de base de datos de las vulnerabilidades de *software*.

Para obtener más información relacionada con la gestión de vulnerabilidades técnicas al utilizar la computación en nube, consulte la serie de Normas 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 la resolución de vulnerabilidades reportadas.

8.9 Gestión de la configuración

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura	#Protección

Control

Se debería establecer, documentar, implementar, monitorizar y revisar todas las configuraciones de *hardware*, *software*, servicios y redes, incluyendo sus configuraciones de seguridad.

Propósito

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.

Orientación

General

La organización debería definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas (incluyendo las configuraciones de seguridad) para *hardware*, *software*, servicios (por ejemplo, servicios en la nube) y redes; tanto para sistemas recién instalados como para sistemas operativos durante su vida útil.

Debería contarse con funciones, responsabilidades y procedimientos para garantizar un control satisfactorio de todos los cambios de configuración.

Plantillas estándar

Se deberían definir plantillas estándar para la configuración segura de *hardware*, *software*, servicios y redes:

a) utilizar directrices disponibles públicamente (por ejemplo, plantillas predefinidas de proveedores y de organizaciones de seguridad independientes);

b) considerar el nivel de protección necesario para determinar un nivel de seguridad suficiente;

c) apoyar la política de seguridad de la información de la organización, las políticas específicas aplicables a casos concretos, las normas 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*.

Para establecer las plantillas estándar para la configuración segura de *hardware*, *software*, servicios y redes, debería considerarse lo siguiente:

a) minimizar el número de identidades con derechos de acceso privilegiados o de nivel de administrador;

b) deshabilitar identidades innecesarias, no utilizadas o inseguras;

c) deshabilitar o restringir funciones y servicios innecesarios;

d) restringir el acceso a herramientas de utilidad potentes y a la configuración de parámetros de host;

e) sincronizar relojes;

f) cambiar la información de autenticación predeterminada por el proveedor, como las contraseñas predeterminadas, inmediatamente después instalación y revisión de otros parámetros importantes relacionados con la seguridad por defecto;

g) configurar el cierre de sesión automático en los dispositivos al transcurrir un tiempo determinado de inactividad de los mismos;

h) verificar que se han cumplido los requisitos de licencia (véase 5.32).

Administración de configuraciones

Debería existir un registro de las configuraciones establecidas de *hardware*, *software*, servicios y redes y mantenerse un registro de todos los cambios de configuraciones. Estos registros deberían almacenarse de forma segura, lo que puede realizarse de varias maneras tales como, bases de datos de configuraciones 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 sea relevante:

a) información actualizada del propietario o punto de contacto del activo;

b) fecha del último cambio de configuración;

c) versión de la plantilla de configuración;

d) relación con las configuraciones de otros activos.

Monitorización de configuraciones

Las configuraciones deberían supervisarse con un conjunto completo de herramientas de administración del sistema (por ejemplo, utilidades de mantenimiento, soporte remoto, herramientas de administración empresarial, *software* de copias de seguridad y restauración) y deberían revisarse regularmente para verificar los ajustes de la 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 bien mediante un análisis manual de la desviación seguido de la aplicación de las acciones correctivas correspondientes.

Información adicional

La documentación para sistemas a menudo contiene detalles sobre la configuración de *hardware* y *software*.

El endurecimiento del sistema es una parte típica de la gestión de la configuración.

La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas.

La automatización suele ser más efectiva para administrar la configuración de seguridad (por ejemplo, usar la infraestructura como código).

Las plantillas de configuración y su destino de aplicación pueden ser información confidencial y deberían protegerse del acceso no autorizado en consecuencia.

8.10 Eliminación de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información #Cumplimiento_jurídico	#Gobernanza_Ecosistema #Resiliencia

Control

La información almacenada en los sistemas de información, en los dispositivos y cualquier otro medio de almacenamiento debería eliminarse cuando ya no sea necesaria.

Propósito

Evitar la exposición innecesaria de información sensible y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de dicha información.

Orientación

General

Con el fin de reducir el riesgo de divulgación no deseada, la información sensible no debería conservarse más tiempo del necesario.

Al momento de eliminar información sobre sistemas, aplicaciones y servicios, hay que tener en consideración lo siguiente:

a) seleccionar un método de eliminación (por ejemplo, sobreescritura electrónica o supresión criptográfica) de acuerdo con los requisitos de la empresa y teniendo en cuenta las leyes y reglamentos aplicables;

b) guardar como evidencia un registro de los resultados de la eliminación de la información;

c) cuando se recurra a proveedores de servicios de eliminación de información, solicitarles pruebas de que la información ha sido eliminada.

Cuando la información de la organización sea almacenada por terceros, la organización debería considerar incluir en los acuerdos con dichos terceros cláusulas relacionadas con la eliminación de dicha información, las cuales deberán aplicarse durante la prestación de dichos servicios y a la finalización de los mismos.

Métodos de borrado

De acuerdo con la política específica de la organización en materia de conservación de datos y teniendo en cuenta la legislación y los reglamentos aplicables, la información sensible debería eliminarse cuando ya no sea necesaria, para lo cual:

a) configurar los sistemas para que eliminen la información de forma segura cuando ya no sea necesaria (por ejemplo, tras un periodo definido sujeto a la política específica de conservación de datos o mediante solicitud de acceso del sujeto);

b) eliminar versiones obsoletas, copias y archivos temporales, dondequiera que se encuentren;

c) utilizar un *software* de borrado seguro aprobado para eliminar permanentemente la información y garantizar que no pueda recuperarse mediante herramientas forenses o de recuperación especializadas;

d) recurrir a aquellos proveedores de servicios de eliminación segura que estén autorizados y certificados;

e) utilizar mecanismos de borrado adecuados para el tipo de soporte de almacenamiento que se va a eliminar (por ejemplo, desmagnetización de unidades de disco duro y otros soportes de almacenamiento magnético).

Cuando se utilicen servicios en la nube, la organización deberá comprobar si el método de supresión proporcionado por el proveedor de servicios en la nube es aceptable y, en caso afirmativo, deberá utilizarlo o bien solicitar al proveedor de servicios en la nube que suprima la información. Estos procesos de eliminación deberían automatizarse de acuerdo con las políticas específicas aplicables al caso concreto, cuando estén disponibles y sean aplicables. Dependiendo de la sensibilidad de la información eliminada, los registros podrán rastrear o verificar que estos procesos de eliminación se han producido.

Para evitar la exposición involuntaria de la información sensible, cuando se devuelven los equipos a los proveedores, la información sensible debería protegerse retirando los almacenamientos auxiliares (por ejemplo, las unidades de disco duro) y la memoria antes de que los equipos salgan de las instalaciones de la organización.

Teniendo en cuenta que el borrado seguro de algunos dispositivos (por ejemplo, los teléfonos inteligentes) sólo puede lograrse 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 adecuado en función de la clasificación de la información manejada por dichos dispositivos.

Deberían aplicarse las medidas de control descritas en el apartado 7.14 para destruir físicamente el dispositivo de almacenamiento y simultáneamente la información que contiene.

Un registro oficial de eliminación de información es útil a la hora de analizar la causa de una posible fuga de la misma.

Información adicional

En la Norma ISO/IEC 27017 se ofrece información sobre la eliminación de datos de usuario en los servicios basados en la nube.

Puede encontrar información sobre la eliminación de datos personales en la Norma ISO/IEC 27555.

8.11 Enmascaramiento de datos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información	#Protección

Control

El enmascaramiento de datos debería utilizarse de acuerdo con la política específica del tema de la organización sobre el control de acceso, con otras políticas específicas relacionadas, así como con los requisitos de negocio, teniendo en cuenta los requisitos legales aplicables.

Propósito

Limitar la exposición de datos sensibles, incluidos los datos de carácter personal y cumplir los requisitos legales, estatutarios, reglamentarios y contractuales.

Orientación

Cuando sea necesario proteger datos personales sensibles, la organización debería considerar la posibilidad de ocultar dichos datos utilizando técnicas como el enmascaramiento de datos, la seudonimización o la anonimización.

Las técnicas de seudonimización o anonimización pueden ocultar los datos personales, disimular la verdadera identidad de los interesados u otra información sensible y eliminar el vínculo entre el responsable del tratamiento y la identidad del titular de la PII o bien el vínculo con otra información sensible.

Cuando se utilicen técnicas de seudonimización o anonimización, debería verificarse que los datos se han seudonimizado o anonimizado correctamente. La anonimización, para que sea eficaz, debería considerar todos los campos de la información sensible. Por ejemplo, si no se tienen en cuenta todos los campos, de forma adecuada, podría llegar a identificarse a una persona, aunque se anonimicen los datos que pueden identificarla directamente, por la presencia de otros datos que permiten identificarla indirectamente.

Otras técnicas de enmascaramiento de datos son:

a) cifrado (que requiera que los usuarios autorizados dispongan de una clave);

b) anulación o supresión de caracteres (para evitar que usuarios no autorizados vean mensajes completos);

c) diferentes números y fechas;

d) sustitución (cambiar un valor por otro para ocultar datos sensibles);

e) sustituir valores por su hash.

A la hora de aplicar técnicas de enmascaramiento de datos, hay que tener en consideración lo siguiente:

a) no conceder acceso a todos los usuarios, a todos los datos personales, diseñar consultas y máscaras para mostrar al usuario sólo aquellos datos personales a los cuales necesita acceder para desarrollar correctamente su trabajo;

b) existen determinados casos en los que algunos datos o registros de una serie de datos, no deberían ser visibles para el usuario; en estos casos, 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 los casos de urgencias, se le muestran, al personal del hospital, los datos parcialmente ofuscados y sólo podrán acceder al resto de datos, aquellos trabajadores con funciones específicas y si, dichos datos, contienen información útil para garantizar un tratamiento adecuado);

c) cuando los datos estén ofuscados, ofrecer al titular de la PII la posibilidad de solicitar que los usuarios no puedan saber si los datos están ofuscados (ofuscación de la ofuscación; esto se utiliza en centros sanitarios, por ejemplo, el paciente no quiere que el personal vea que se ha ofuscado información sensible como embarazos o resultados de análisis de sangre);

d) cualquier requisito legal o reglamentario (por ejemplo, que exija enmascarar la información de las tarjetas de pago durante su procesamiento o almacenamiento).

Al utilizar el enmascaramiento, la seudonimización o la anonimización de datos, debería tenerse en cuenta lo siguiente:

a) nivel de fortaleza del enmascaramiento, la seudonimización o la anonimización de los datos, en función del uso de dichos datos;

b) controlar el acceso al tratamiento de datos;

c) acuerdos o restricciones sobre el tratamiento de datos;

d) la prohibición de cotejar los datos tratados con otra información, con el fin de identificar al titular de la PII;

e) seguimiento de la recogida y recepción de los datos tratados.

Información adicional

La anonimización altera de forma irreversible los datos personales, de tal manera que el titular de la PII ya no puede ser identificado directa o indirectamente.

La seudonimización sustituye la información identificativa por un alias. Conocer el algoritmo (a veces denominado "información adicional") utilizado para llevar a cabo la seudonimización permite una forma de identificación del titular de la PII. Por lo tanto, dicha "información adicional" debería mantenerse separada y protegida.

Aunque la seudonimización es, por lo tanto, más débil que la anonimización, los conjuntos de datos seudonimizados pueden ser más útiles en la investigación estadística.

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar datos sensibles. El enmascaramiento de datos puede ser estático (cuando los elementos de datos se enmascaran en la base de datos original), dinámico (utilizando automatización y reglas para asegurar los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

Las funciones hash pueden utilizarse para anonimizar datos personales. Para evitar ataques de enumeración, siempre deberían combinarse con una función "salt".

Debería evitarse el uso de datos personales, en los identificadores de recursos y sus atributos [por ejemplo, nombres de archivo, localizadores uniformes de recursos (URL)] o anonimizarse adecuadamente.

En la Norma ISO/IEC 27018 figuran controles adicionales relativos a la protección de datos personales en nubes públicas.

Para más información sobre las técnicas de desidentificación, consulte la Norma ISO/IEC 20889.

8.12 Prevención de fugas de datos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad	#Proteger #Detectar	#Protección_de_la_información	#Protección #Defensa

Control

Se deberían aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

Propósito

Detectar e impedir la divulgación y extracción no autorizadas de información por parte de personas o sistemas.

Orientación

Para reducir el riesgo de fuga de datos, la organización debería tener en consideración lo siguiente:

a) identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos);

b) monitorizar los canales por los cuales pueda producirse una fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles);

c) tomar acciones para evitar que se filtre información (por ejemplo, poner en cuarentena los correos electrónicos que contengan información sensible).

Las herramientas de prevención de fuga de datos deberían utilizarse para:

a) identificar y controlar la información sensible que corre el riesgo de ser divulgada sin autorización (por ejemplo, en datos no estructurados del sistema de un usuario);

b) detectar la divulgación de información sensible (por ejemplo, cuando la información se carga en servicios en la nube de terceros no fiables o se envía por correo electrónico);

c) bloquear acciones del usuario o transmisiones de red que expongan información sensible (por ejemplo, impedir que se copien entradas de una 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 bien cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización. Si este fuera el caso, la organización debería implementar tecnología necesaria, tales como herramientas de prevención de fuga de datos o bien configurar las herramientas con las que cuente, de forma tal, que permitan a los usuarios ver y manipular la información de forma remota, pero que impidan su copiado y pegado, fuera de la fuera del control de la organización.

Si es necesario exportar datos, el propietario de dichos datos debería poder aprobar la exportación y responsabilizar a los usuarios de sus acciones.

Las capturas de pantalla o fotografías de la pantalla se deberían abordarse mediante condiciones de uso, formación y auditorias.

Cuando se realicen copias de seguridad de los datos, hay que asegurarse de que la información sensible está protegida con medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad.

También se debería considerar la prevención contra la fuga de datos como protección contra las acciones de inteligencia de un adversario para obtener información confidencial o secreta (geopolítica, humana, financiera, comercial, científica o de cualquier otro tipo) que pueda ser de interés para el espionaje o bien pueda ser crítica para la comunidad. Las acciones de prevención de fuga de datos deberían estar orientadas a confundir las decisiones del adversario, por ejemplo sustituyendo información auténtica por información falsa, ya sea como acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de “honeypots” para atraer a los atacantes.

Información adicional

Las herramientas para la prevención de fuga de datos, están diseñadas para identificar datos, supervisar su uso y movimiento y tomar medidas para evitar que se filtren (por ejemplo, alertando a los usuarios de su comportamiento arriesgado y bloqueando la transferencia de datos a dispositivos de almacenamiento portátiles).

La prevención contra la fuga de datos implica, intrínsecamente, el control de las comunicaciones y actividades en línea del personal y, por extensión, de los mensajes de terceros, lo que plantea problemas legales que deberían tenerse en cuenta antes de desplegar las herramientas de prevención de la fuga de datos. Existe una variedad de legislación relativa a la privacidad, la protección de datos, el empleo, la interceptación de datos y las telecomunicaciones que es aplicable a la supervisión y al tratamiento de datos en el contexto de la prevención de fuga de datos.

La prevención contra la fuga de datos puede apoyarse en controles de seguridad estándar, como políticas específicas sobre control de acceso y gestión segura de documentos (véanse 5.12 y 5.15).

8.3 Copias de seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Protección

Control

Las copias de seguridad de la información, del *software* y de los sistemas deberían mantenerse y probarse periódicamente de acuerdo con la política de copias de seguridad específica acordada.

Propósito

Permitir la recuperación tras la pérdida de datos o sistemas.

Orientación

Debería establecerse una política específica de copias de seguridad para abordar los requisitos de conservación de datos y seguridad de la información de la organización.

Deberían proporcionarse instalaciones adecuadas para las copia de seguridad con el fin de garantizar que toda la información y *software* esenciales puedan recuperarse tras un incidente o fallo o pérdida de medios de almacenamiento.

Deberían desarrollarse e implementarse planes sobre cómo la organización realizará copias de seguridad de la información, el *software* y los sistemas, para abordar la política específica sobre copias de seguridad.

A la hora de diseñar un plan de copias de seguridad, debería tenerse en cuenta los siguientes aspectos:

a) elaborar registros precisos y completos de las copias de seguridad y de los procedimientos de restauración documentados;

b) reflejar los requisitos de negocio de la organización (por ejemplo, el objetivo del punto de recuperación o RPO, véase 5.30), los requisitos de seguridad de la información implicada y la criticidad de la información para el funcionamiento continuo de la organización (por ejemplo, copia de seguridad completa o diferencial) y la frecuencia de realización de las copias de seguridad;

c) almacenar las copias de seguridad en una ubicación remota, segura y protegida, a una distancia suficiente para evitar cualquier daño provocado por un desastre en el sitio principal;

d) dotar, a la copia de seguridad, de un nivel adecuado de protección física y medioambiental (véanse el capítulo 7 y 8.1) coherente con las normas aplicadas en el emplazamiento principal;

e) realizar pruebas periódicas de los soportes que almacenan las copias de seguridad, para garantizar que pueden utilizarse cuando sea necesario. Probar la capacidad de restaurar los datos de las copias de seguridad en un sistema de prueba, no sobrescribiendo el soporte de almacenamiento original en caso de que el proceso de copia de seguridad o la restauración falle y cause daños o pérdidas irreparables de datos;

f) proteger las copias de seguridad mediante cifrado en función de los riesgos identificados (por ejemplo, en situaciones en las que la confidencialidad es importante);

g) asegurarse de que se detecta una pérdida involuntaria de datos antes de realizar la copia de seguridad.

Los procedimientos operacionales deberían supervisar la ejecución de las copias de seguridad y abordar los fallos de las copias de seguridad programadas para garantizar la integridad de las mismas de acuerdo con la política aplicable de copias de seguridad.

Las medidas aplicables a las copias de seguridad de los sistemas y los servicios individuales deberían probarse periódicamente, para garantizar que cumplen los objetivos contenidos en los planes de respuesta a incidentes y de continuidad de la actividad (véase 5.30). Esto debería combinarse con una prueba de los procedimientos de restauración y cotejarse con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de los sistemas y servicios críticos, las medidas de copia de seguridad deberían cubrir toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de catástrofe.

Cuando la organización utiliza un servicio en la nube, se deberían realizar copias de seguridad de la información, de las aplicaciones y de los sistemas de la organización en el entorno del servicio en la nube. La organización debería determinar si se cumplen los requisitos para la realización de copias de seguridad cuando se utiliza el servicio de copia de seguridad de la información proporcionado como parte del servicio en la nube, y cómo.

Debería determinarse el periodo de conservación de la información empresarial esencial, teniendo en cuenta cualquier requisito de conservación de copias de archivo. La organización debería considerar la eliminación de la información (véase 8.10) en los medios de almacenamiento utilizados para las copias de seguridad una vez que expire el período de conservación de la información, teniendo en cuenta la legislación y la normativa aplicable.

Información adicional

Para más información sobre la seguridad del almacenamiento, incluida la consideración de la conservación, véase la Norma ISO/IEC 27040.

8.14 Redundancia de los recursos de tratamiento de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Disponibilidad	#Proteger	#Continuidad #Gestión_de_activos	#Protección #Resiliencia

Control

Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

Propósito

Garantizar el funcionamiento continuo de las instalaciones de tratamiento de la información.

Orientación

La organización debería identificar los requisitos para la disponibilidad de los servicios empresariales y los sistemas de información. La organización debería diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir estos requisitos.

La redundancia puede implementarse duplicando las instalaciones de tratamiento de la información, en parte o en su totalidad (es decir, componentes de repuesto o tener dos de todo). La organización debería planificar y aplicar procedimientos para activar los componentes e instalaciones de procesamiento redundantes. Los procedimientos deberían establecer si los componentes redundantes y las actividades de procesamiento se activan siempre o, en caso de emergencia, se activan de forma automática o manual. Los componentes redundantes y las instalaciones de tratamiento de la información deberían garantizar el mismo nivel de seguridad que los primarios.

Deberían existir mecanismos para alertar a la organización de cualquier fallo en las instalaciones de tratamiento de la información, permitir la ejecución del procedimiento previsto y mantener la disponibilidad mientras se reparan o sustituyen las instalaciones de tratamiento de la información.

La organización debería tener en consideración lo siguiente a la hora de implementarse sistemas redundantes:

a) contratar dos o más proveedores de red y de instalaciones de tratamiento de la información crítica, tales como proveedores de servicios de Internet;

b) utilizar redes redundantes;

c) utilizar dos centros de datos separados geográficamente, con sistemas duplicados;

d) utilizar fuentes de alimentación físicas redundantes;

e) utilizar instancias paralelas múltiples de componentes de *software*, con balanceo de carga automático entre ellas (entre instancias en el mismo centro de datos o en centros de datos diferentes);

f) duplicar componentes en sistemas (por ejemplo, CPU, discos duros, memorias) o en redes (por ejemplo, cortafuegos, enrutadores, conmutadores).

Cuando proceda, preferiblemente en modo de producción, los sistemas de información redundantes deberían probarse para garantizar que la conmutación de un componente a otro, cuando sucede algún error, funciona según lo previsto.

Información adicional

Existe una estrecha 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 redundancia pueden formar parte de las estrategias y soluciones de continuidad de las TIC.

La implementación de redundancias puede introducir riesgos para la integridad (por ejemplo, los procesos de copia de datos en componentes duplicados pueden introducir errores) o para la confidencialidad (por ejemplo, un control de seguridad deficiente de los componentes duplicados puede llevar a un compromiso) de la información y de los sistemas de información; que deben tenerse en cuenta a la hora de diseñar los sistemas de información.

La redundancia en las instalaciones de tratamiento de la información no suele abordar la falta de disponibilidad de las aplicaciones, debida a fallos dentro de una aplicación.

Con el uso de la computación en la nube pública, es posible tener múltiples versiones vivas de las instalaciones de tratamiento de la información, que existen en múltiples ubicaciones físicas separadas con conmutación por error automática y balanceo de carga entre ellas.

Algunas de las tecnologías y técnicas para proporcionar redundancia y conmutación automática por error en el contexto de los servicios en nube se tratan en la Norma ISO/IEC TS 23167.

8.15 Registros de eventos

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Protección #Defensa

Control

Se deberían generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.

Propósito

Para registrar eventos, generar evidencias, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y apoyar las investigaciones.

Orientación

General

La organización debería determinar el propósito para el que se crean los registros, qué datos se recopilan y registran, y cualquier requisito específico de registro para proteger y manejar los datos de registro. Esto debería documentarse en una política específica sobre el registro.

Los registros de eventos deberían incluir para cada evento, según corresponda:

a) ID de usuario;

b) actividades del sistema;

c) fechas, horas y detalles de eventos relevantes (por ejemplo, inicio de sesión y cierre de sesión);

d) la identidad del dispositivo, el identificador del sistema y la ubicación;

e) direcciones y protocolos de red.

Se deberían considerar los siguientes eventos para el registro:

a) intentos exitosos y rechazados de acceso al sistema;

b) los datos exitosos y rechazados y otros intentos de acceso a recursos;

c) cambios en la configuración del sistema;

d) uso de privilegios;

e) el uso de programas y aplicaciones de utilidad;

f) los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;

g) alarmas emitidas por el sistema de control de acceso;

h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de detección de intrusiones;

i) creación, modificación o supresión de identidades;

j) transacciones ejecutadas por usuarios en aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o 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 registros entre sistemas para análisis, alerta e investigación de un incidente.

Protección de los registros

Los usuarios, incluidos con derechos de acceso privilegiados, no deberían tener permiso para eliminar o desactivar los registros de sus propias actividades. Potencialmente pueden manipular los registros de las instalaciones de tratamiento de la información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios privilegiados.

Los controles deberían tener como objetivo proteger contra cambios no autorizados en la información de registro y problemas operacionales con la instalación de registros, incluyendo:

a) alteraciones en los tipos de mensajes que se registran;

b) edición o eliminación de archivos de registros.

c) la falta de registro de eventos o la sobreescritura de eventos registrados anteriores si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de los registros, se debería considerar el uso de las siguientes técnicas: *hashing* criptográfico, grabación en un archivo de solo apéndice y solo lectura, grabación en un archivo de transparencia pública.

Algunos registros de auditoría pueden ser necesarios para ser archivados debido a los requisitos de retención de datos o requisitos para recopilar y retener pruebas (véase 5.28).

Cuando la organización necesite enviar registros de sistemas o aplicaciones a un proveedor para ayudar con errores de depuración o resolución de problemas, los registros deberían anonimizarse cuando sea posible utilizando técnicas de enmascaramiento de datos (véase 8.11) para información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlos al proveedor.

Los registros de eventos pueden contener datos confidenciales e información personal identificable. Deberían adoptarse medidas adecuadas de protección de la intimidad (véase 5.34).

Análisis de registro

El análisis de registros debería abarcar el análisis e interpretación de eventos de seguridad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso.

El análisis de los acontecimientos debería realizarse teniendo en cuenta:

a) las habilidades necesarias para los expertos que realizan el análisis;

b) determinar el procedimiento de análisis del registro;

c) los atributos requeridos de cada evento relacionado con la seguridad;

d) las excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, información de seguridad y gestión de eventos (SIEM) o reglas de firewall, y sistemas de detección de intrusiones (IDS) o firmas de código malicioso];

e) patrones de comportamiento conocidos y tráfico de red estándar en comparación con la actividad y el comportamiento anómalos [análisis del comportamiento de los usuarios y entidades (UEBA)];

f) resultados del análisis de tendencias o patrones (por ejemplo, como resultado de la utilización de análisis de datos, técnicas de macrodatos 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 el comportamiento anómalo, que incluye:

a) revisar los intentos exitosos y fallidos de acceder a recursos protegidos [por ejemplo, servidores del sistema de nombres de dominio (DNS), portales web y archivos compartidos];

b) comprobar los registros DNS para identificar conexiones de red salientes a servidores maliciosos, como los asociados con los servidores de comando y control de redes de equipos infectados;

c) examinar los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicios) para actividades inusuales dentro de los sistemas y redes (por ejemplo, revisando los patrones de actividad);

d) incluyendo registros de eventos de monitoreo físico, como entrada y salida, para garantizar una detección y un análisis de incidentes más precisos;

e) correlacionar registros para permitir un análisis eficiente y altamente preciso.

Los incidentes de seguridad de la información especificados y reales deberían ser identificados (por ejemplo, infección de código malicioso o sondeo de firewalls) y ser objeto de una investigación adicional (por ejemplo, como parte de un proceso de gestión de incidentes de seguridad de la información, véase 5.25).

Información adicional

Los registros del sistema a menudo contienen un gran volumen de información, gran parte de la cual es ajena al monitoreo de seguridad de la información. Para ayudar a identificar eventos significativos para fines de monitoreo de seguridad de la información, se puede considerar el uso de programas de utilidad adecuados o herramientas de auditoría para interrogar los archivos.

El registro de eventos sienta las bases para los sistemas de monitoreo automatizados (véase 8.16) que son capaces de generar informes y alertas consolidados sobre la seguridad del sistema.

Una herramienta SIEM o servicio equivalente se puede utilizar para almacenar, correlacionar, normalizar y analizar información de registro**,** y para generar alertas. Los SIEM tienden a requerir una configuración cuidadosa para optimizar sus beneficios. Las configuraciones para considerar incluyen la identificación y selección de fuentes de registro apropiadas, el ajuste y la prueba de reglas y el desarrollo de casos de uso.

Los archivos de transparencia pública para el registro de registros se utilizan, por ejemplo, en los sistemas de transparencia de certificados. Estos archivos pueden proporcionar un mecanismo de detección adicional útil para proteger contra la manipulación de registros.

En entornos de nube, las responsabilidades de administración de registros se pueden compartir entre el cliente de servicio en la nube y el proveedor de servicios en la nube. Las responsabilidades varían según el tipo de servicio en la nube que se utilice. Puede encontrar más orientación en la Norma ISO/IEC 27017.

8.16 Seguimiento de actividades

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	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 monitorizarse en busca de comportamientos anómalos y se deberían tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

Propósito

Detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

Orientación

El alcance y el nivel de supervisión deberían determinarse de conformidad con los requisitos de seguridad empresarial y de la información y teniendo en cuenta las leyes y reglamentos pertinentes. Los registros de seguimiento deberían mantenerse durante períodos de retención definidos.

Deberían tenerse en cuenta para su inclusión en el sistema de seguimiento lo siguiente:

a) tráfico de la red, el sistema y la aplicación salientes y entrantes;

b) acceso a sistemas, servidores, equipos de red, sistemas de monitoreo, aplicaciones críticas, etc.;

c) archivos de configuración de red y sistemas críticos o de nivel de administración;

d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, firewalls, prevención de fugas 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 a ejecutarse en el sistema y que no ha sido manipulado (por ejemplo, mediante el recompilado para agregar código no deseado adicional);

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 supervisar esta línea de base para detectar anomalías. Al establecer una línea de base, se considerará lo siguiente:

a) revisar la utilización de los sistemas en períodos normales y picos;

b) hora habitual de acceso, ubicación del acceso, frecuencia de acceso para cada usuario o grupo de usuarios;

El sistema de seguimiento debería configurarse con arreglo a la línea de base establecida para identificar comportamientos anómalos, tales como:

a) terminación no planificada de procesos o solicitudes;

b) actividad típicamente asociada con código malicioso o tráfico originado por direcciones IP maliciosas conocidas o dominios de red (por ejemplo, aquellos asociados con servidores de comando y control de red de equipos infectados);

c) características de ataque conocidas (por ejemplo, denegación de servicio y desbordamientos 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, cola de red, niveles de latencia y agitación de la red);

f) el acceso no autorizado (real o intentado) a sistemas o información;

g) escaneo no autorizado de aplicaciones, sistemas y redes empresariales;

h) intentos exitosos y fallidos de 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.

Debería utilizarse un seguimiento continuo a través de una herramienta de seguimiento. El monitoreo debería realizarse 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 la notificación en tiempo real. Las herramientas también deberían ser capaces de reconocer firmas y datos específicos o patrones de comportamiento de redes o aplicaciones.

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) en función de umbrales predefinidos. El sistema de alerta debería ser sintonizado y entrenado en la línea de base de la organización para minimizar los falsos positivos. El personal debería dedicarse a responder a las alertas y debería estar debidamente capacitado para interpretar con precisión los posibles incidentes. Debería haber sistemas y procesos redundantes para recibir y responder a las notificaciones de alerta.

Los acontecimientos anormales deberían comunicarse a las partes pertinentes con el fin de mejorar las siguientes actividades: auditoría, evaluación de seguridad, análisis y monitoreo de vulnerabilidades (véase 5.25). Deberían establecerse procedimientos para responder oportunamente a los indicadores positivos del sistema de seguimiento, a fin de reducir al mínimo el efecto de los acontecimientos adversos (véase 5.26) sobre la seguridad de la información. También deberían establecerse procedimientos para identificar y abordar los falsos positivos, incluida la puesta a punto del *software* de seguimiento para reducir el número de falsos positivos futuros.

Información adicional

El monitoreo de seguridad se puede mejorar mediante:

a) aprovechamiento de los sistemas de inteligencia de amenazas (véase 5.7);

b) aprovechar las capacidades de aprendizaje automático e inteligencia artificial;

c) utilizando listas de bloqueo o listas permitidas.

d) realizar una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidades, pruebas de penetración, simulaciones de ciberataques y ejercicios de respuesta cibernética), y utilizar los resultados de estas evaluaciones para ayudar a determinar las bases de referencia o el comportamiento aceptable;

e) utilizar sistemas de control del rendimiento para ayudar a establecer y detectar comportamientos anómalos;

f) aprovechar los registros en combinación con los sistemas de monitoreo.

Las actividades de monitoreo a menudo se llevan a cabo utilizando *software* especializado, como sistemas de detección de intrusiones. Estos se pueden configurar para una línea de base de las actividades normales, aceptables y esperadas del sistema y la red.

El monitoreo de comunicaciones anómalas ayuda en la identificación de redes de equipos infectados (es decir, conjunto de dispositivos bajo el control malicioso del propietario de la red de equipos infectados, generalmente utilizado para montar ataques distribuidos de denegación de servicio en otras computadoras de otras organizaciones). Si el equipo está siendo controlado por un dispositivo externo, hay una comunicación entre el dispositivo infectado y el controlador.

Por lo tanto, la organización debería emplear tecnologías para supervisar las comunicaciones anómalas y tomar las medidas necesarias.

8.17 Sincronización del reloj

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	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 con fuentes de tiempo aprobadas.

Propósito

Deberían permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y apoyar las investigaciones sobre incidentes de seguridad de la información.

Orientación

Los requisitos externos e internos para la representación del tiempo, la sincronización fiable y la precisión deberían documentarse e implementarse. Estos requisitos pueden provenir de necesidades legales, estatutarias, reglamentarias, contractuales, de normas y de supervisión interna. Se deberían definir y considerar un tiempo de referencia estándar para su uso dentro de la organización para todos los sistemas, incluidos los sistemas de gestión de edificios, los sistemas de entrada y salida y otros que puedan utilizarse para ayudar a las investigaciones.

Un reloj vinculado a un tiempo de radio transmitido 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 de fecha y hora consistente y confiable para garantizar sellos de tiempo precisos. Protocolos como el protocolo de tiempo de red (NTP) o el protocolo de tiempo de precisión (PTP) deberían usarse para mantener todos los sistemas en red en sincronización con un reloj de referencia.

La organización puede utilizar dos fuentes de tiempo externas al mismo tiempo con el fin de mejorar la fiabilidad de los relojes externos, y gestionar adecuadamente cualquier varianza.

La sincronización del reloj puede ser difícil cuando se utilizan múltiples servicios en la nube o cuando se utilizan servicios tanto en la nube como en las instalaciones. En este caso, el reloj de cada servicio debería ser monitoreado y la diferencia registrada con el fin de mitigar los riesgos derivados de las discrepancias.

Información adicional

El ajuste correcto de los relojes de computadora es importante para garantizar la precisión de los registros de eventos, que pueden ser necesarios para investigaciones o como evidencia en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar tales investigaciones y dañar la credibilidad de dichas pruebas.

8.18 Uso de los programas de utilidad con privilegios

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_de_la_red #Configuración_segura #Seguridad_de_las_aplicaciones	#Protección

Control

Se deberían restringir y controlar rigurosamente el uso de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

Propósito

Garantizar que el uso de programas de utilidades no perjudique los controles del sistema y de las aplicaciones para la seguridad de la información.

Orientación

Se deberían considerar las siguientes pautas para el uso de programas de utilidad que pueden ser capaces de controlar el sistema y la aplicación:

a) limitación del uso de programas de utilidad al número mínimo práctico de usuarios autorizados de confianza (véase 8.2);

b) el uso de procedimientos de identificación, autenticación y autorización para programas de utilidad, incluida la identificación única de la persona que utiliza el programa de utilidad;

c) definir y documentar los niveles de autorización para programas de servicios públicos;

d) autorización para el uso ad hoc de programas de utilidad;

e) no poner programas de utilidad a disposición de los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere la segregación de deberes;

f) eliminar o deshabilitar todos los programas de utilidad innecesarios;

g) como mínimo, la segregación 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 programas de utilidad (por ejemplo, durante la duración de un cambio autorizado);

i) registro de todo uso de programas de utilidad.

Información adicional

La mayoría de los sistemas de información tienen uno o más programas de utilidad que pueden ser capaces de anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, copias de seguridad y herramientas de red.

8.19 Instalación del software en sistemas de producción

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad del sistema y de la red #Configuración segura #Seguridad de las aplicaciones	#Protección

Control

Deberían implementarse procedimientos y medidas para gestionar de forma segura la instalación de *software* en los sistemas en producción.

Propósito

Garantizar la integridad de los sistemas operacionales y evitar la explotación de vulnerabilidades técnicas.

Orientación

Se deberían considerar las siguientes directrices para gestionar de forma segura los cambios y la instalación de programas informáticos en los sistemas operacionales:

a) realizar actualizaciones de *software* operacional solo por administradores capacitados con la autorización de gestión adecuada (véase 8.5);

b) garantizar que en los sistemas operacionales solo se instale código ejecutable aprobado y ningún código de desarrollo o compiladores;

c) instalar y actualizar *software* únicamente después de pruebas extensas y exitosas (véanse 8.29 y 8.31);

d) actualizar todas las bibliotecas de origen del programa correspondientes;

e) utilizar un sistema de control de configuración para mantener el control de todo el *software* operacional, así como la documentación del sistema;

f) definir una estrategia de retroceso antes de que se implementen los cambios;

g) mantener un registro de auditoría de todas las actualizaciones del *software* operacional;

h) archivar versiones antiguas del *software*, junto con toda la información y parámetros requeridos, procedimientos, detalles de configuración y *software* de soporte como medida de contingencia, y mientras el *software* sea necesario para leer o procesar datos archivados.

Cualquier decisión de actualizar a una nueva versión debería tener en cuenta los requisitos comerciales para el cambio y la seguridad de la versión (por ejemplo, la introducción de nuevas funciones de seguridad de la información o el número y la gravedad de las vulnerabilidades de seguridad de la información que afectan a la versión actual). Los parches de *software* deberían aplicarse cuando pueden ayudar a eliminar o reducir las vulnerabilidades de seguridad de la información (véanse 8.8 y 8.19).

El *software* informático puede basarse en *software* y paquetes suministrados externamente (por ejemplo, programas de *software* que utilizan módulos 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 utilizado en los sistemas operacionales debería mantenerse a un nivel de soporte por el proveedor. Con el tiempo, los proveedores de *software* dejarán de admitir versiones anteriores de *software*. La organización debería considerar los riesgos de confiar en *software* sin soporte. El *software* de código abierto utilizado en los sistemas operativos debería mantenerse hasta la última versión apropiada del *software*. Con el tiempo, el código fuente abierto puede dejar de mantenerse, pero todavía está disponible en un repositorio de *software* de código abierto. La organización también debería considerar los riesgos de confiar en *software* de código abierto no mantenido cuando se utiliza en sistemas operacionales.

Cuando los proveedores participan en la instalación o actualización de *software*, el acceso físico o lógico solo debería darse cuando sea necesario y con la autorización adecuada. Las actividades del proveedor deberían ser objeto de seguimiento (véase 5.22).

La organización debería definir y hacer cumplir reglas estrictas sobre qué tipos de *software* pueden los usuarios instalar.

El principio de privilegio mínimo debería aplicarse a la instalación de *software* en sistemas operacionales. La organización debería identificar qué tipos de instalaciones de *software* están permitidas (por ejemplo, actualizaciones y parches de seguridad del *software* existente) y qué tipos de instalaciones están prohibidas (por ejemplo, *software* que es solo para uso personal y *software* cuyos antecedentes con respecto a ser potencialmente malicioso son desconocidos o sospechosos). Estos privilegios deberían concederse en función de las funciones de los usuarios afectados.

Información adicional

Ninguna información adicional.

8.20 Seguridad de redes

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad del sistema y de la red	#Protección

Control

Las redes y los dispositivos de red deberían ser securizados, gestionados y controlados para proteger la información en los sistemas y aplicaciones.

Propósito

Garantizar la seguridad en el uso de los servicios de red y de sus instalaciones de tratamiento de la información de apoyo frente a riesgos a través de la red.

Orientación

Deberían aplicarse controles para garantizar la seguridad de la información en las redes y proteger los servicios conectados del acceso no autorizado. En particular, deberían tenerse en cuenta los siguientes puntos:

a) el tipo y nivel de clasificación de la información que la red puede soportar;

b) establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red;

c) mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos (por ejemplo, enrutadores, conmutadores);

d) separar la responsabilidad operativa de las redes de las operaciones de los sistemas de TIC cuando proceda (véase 5.3);

e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceros o redes inalámbricas y para proteger las redes y aplicaciones conectadas (véanse 5.22, 8.24, 5.14 y 6.6). También pueden exigirse controles adicionales para mantener la disponibilidad de los servicios de red y los ordenadores conectados a la red;

f) el registro y el seguimiento adecuados para permitir el registro y la detección de acciones que puedan afectar o sean pertinentes a la seguridad de la información (véanse 8.16 y 8.15);

g) coordinar estrechamente las actividades de gestión de la red, tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de información.

h) autenticación de los sistemas en la red;

i) restringir y filtrar la conexión de los sistemas a la red (por ejemplo, utilizando firewalls);

j) detectar, restringir y autenticar la conexión de equipos y dispositivos a la red;

k) bastionado de los dispositivos de red;

l) segregar los canales de administración de red de otros tráficos de red;

m) aislar temporalmente subredes críticas (por ejemplo, con puentes levadizos) si la red está bajo ataque;

n) desactivación de protocolos de red vulnerables.

La organización debería garantizar que se apliquen controles de seguridad adecuados al uso de redes virtualizadas. Las redes virtualizadas también cubren redes definidas por *software* (SDN, SD-WAN). Las redes virtualizadas pueden ser deseables desde el punto de vista de la seguridad, ya que pueden permitir la separación lógica de la comunicación sobre las redes físicas, particularmente para los sistemas y aplicaciones que se implementan utilizando la computación distribuida.

Información adicional

Puede encontrar información adicional sobre la seguridad de la red en la serie ISO/IEC 27033.

Puede encontrar más información sobre las redes virtualizadas en la Especificación Técnica ISO/IEC TS 23167.

8.21 Seguridad de los servicios de red

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad del sistema y de la red	#Protección

Control

Se deberían identificar, implementar y monitorizar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de todos los servicios de red.

Propósito

Garantizar la seguridad en el uso de los servicios de la red.

Orientación

Las medidas de seguridad necesarias para determinados servicios, como las características de seguridad, los niveles de servicio y los requisitos de servicio, deberían identificarse y aplicarse (por parte de proveedores de servicios de red internos o externos). La organización debería garantizar que los proveedores de servicios de red implementen estas medidas.

Debería determinarse y supervisarse periódicamente la capacidad del proveedor de servicios de red para gestionar los servicios acordados de manera segura. El derecho a la auditoría debería acordarse entre la organización y el proveedor. La organización también debería considerar los certificados de terceros proporcionados por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Las normas sobre el uso de redes y servicios de red deberían formularse y aplicarse para abarcar:

a) las redes y servicios de red a los que se permite acceder;

b) requisitos de autenticación para acceder a varios servicios de red;

c) procedimientos de autorización para determinar quién está autorizado a acceder a qué redes y redes;

d) gestión de redes y controles y procedimientos tecnológicos para proteger el acceso a las conexiones de red y a los servicios de red;

e) los medios utilizados para acceder a las redes y los servicios de red [por ejemplo, el uso de la red privada virtual (VPN) o la red inalámbrica];

f) tiempo, ubicación y otros atributos del usuario en el momento del acceso;

g) seguimiento del uso de los servicios de red.

Deberían tenerse en cuenta las siguientes características de seguridad de los servicios de red:

a) tecnología aplicada para la seguridad de los servicios de red, como la autenticación, el cifrado y los controles de conexión de red;

b) parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de seguridad y conexión de 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 del servicio de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.

Información adicional

Los servicios de red incluyen el suministro de conexiones, servicios de red privada y soluciones de seguridad de red gestionadas, como firewalls y sistemas de detección de intrusiones. Estos servicios pueden ir desde simples anchos de banda no administrados hasta ofertas complejas de valor agregado.

En la Norma ISO/IEC 29146, se ofrecen más orientaciones sobre un marco para la gestión del acceso.

8.22 Segregación en redes

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad del sistema y de la red	#Protección

Control

Los grupos de servicios de información, de usuarios y de sistemas de información deberían ser segregados en las redes de la organización.

Propósito

Dividir la red en los límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de negocio.

Orientación

La organización debería considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separarlas 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 bajo y alto riesgo), a lo largo de las unidades organizativas (por ejemplo, recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio del servidor que se conecta a varias unidades organizativas). La segregación se puede hacer usando redes físicamente diferentes o mediante el uso de 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 utilizando una puerta de enlace (por ejemplo, firewall, enrutador de filtrado). Los criterios para la agregación de redes en dominios, y el acceso permitido a través de las pasarelas, debería basarse en una evaluación de los requisitos de seguridad de cada dominio. La evaluación debería ajustarse a la política específica en materia de control del acceso (véase 5.15), los requisitos de acceso, el valor y la clasificación de la información procesada y tener en cuenta el impacto relativo en el coste y el rendimiento de la incorporación de una tecnología de pasarela adecuada.

Las redes inalámbricas requieren un tratamiento especial debido a su perímetro de red mal definido. El ajuste de la cobertura de radio debería considerarse para la segregación de las redes inalámbricas. Para los entornos sensibles, debería tenerse en cuenta tratar todo el acceso inalámbrico como conexiones externas y separar este acceso de las redes internas hasta que el acceso haya pasado a través de una pasarela de acuerdo con los controles de red (véase 8.20) antes de conceder el acceso a los sistemas internos. La red de acceso inalámbrico para los invitados debería separarse de las del personal si el personal solo utiliza dispositivos finales de usuario controlados que cumplan con las políticas específicas de la organización. La red WiFi para los invitados debería tener al menos las mismas restricciones que la red WiFi para el personal, con el fin de desalentar el uso de la red WiFi de invitados por el personal.

Información adicional

Las redes a menudo se extienden más allá de los límites de la organización, ya que se forman asociaciones comerciales que requieren la interconexión o el intercambio de instalaciones de procesamiento de información y redes. Tales extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que utilizan la red, algunas de las cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.

8.23 Filtrado de webs

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad del sistema y de la red	#Protección

Control

El acceso a sitios web externos debería gestionarse para reducir la exposición a contenido malicioso.

Propósito

Proteger que los sistemas sean comprometidos por código malicioso y para prevenir el acceso a recursos web no autorizados.

Orientación

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 del sitio web en cuestión. Algunos navegadores y tecnologías antimalware lo hacen automáticamente o se pueden configurar 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 tengan una función de subida de información a menos que se permita por válidas razones de negocio;

b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen contenido malicioso o phishing);

c) Servidores de comando y control;

d) sitio web malicioso adquirido a partir de la 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 indeseables o inapropiados y aplicaciones basadas en la web. Las normas deberían mantenerse actualizadas.

Debería impartirse capacitación al personal sobre el uso seguro y adecuado 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 sea necesario acceder a recursos web restringidos por legítimas razones de negocio. También debería impartirse capacitación al personal para garantizar que no anule ningún aviso del navegador que informe de que un sitio web no es seguro, pero que permite al usuario proceder.

Información adicional

El filtrado web puede incluir una gama de técnicas que incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración a medida para ayudar a evitar que el código malicioso y otras actividades maliciosas ataquen la red y los sistemas de la organización.

8.24 Uso de la criptografía

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	# Proteger	#Configuración_segura	#Proteger

Control

Debería definirse e implementarse reglas para el uso eficaz de la criptografía, incluida para la gestión de claves criptográficas.

Propósito

Garantizar un uso efectivo y adecuado de la criptografía para proteger la confidencialidad, autenticidad o la integridad de la información de acuerdo con los requisitos de negocio y de seguridad de la información, y tomando en consideración los requisitos legales, estatutarios, regulatorios y contractuales relativos a la criptografía.

Orientación

General

Cuando se use la criptografía, debería considerarse lo siguiente:

a) la política específica definida por la organización en materia de criptografía, incluyendo los principios generales para la protección de la información. Una política específica en esta materia es necesaria para maximizar los beneficios y minimizar los riesgos del uso de las técnicas criptográficas y para evitar un uso incorrecto o inapropiado;

b) la identificación del nivel requerido de protección y la clasificación de la información y, consecuentemente, el establecimiento del tipo, fortaleza y calidad de los algoritmos criptográficos requeridos;

c) el uso de la criptografía para la protección de la información almacenada en los dispositivos finales móviles de los usuarios o en medios de almacenamiento y transmitida a través de las redes a estos dispositivos o medios de almacenamiento;

d) la aproximación a la gestión de claves, incluyendo los métodos para la generación y protección de las claves criptográficas y la recuperación de la información cifrada en caso de pérdida, compromiso o cuando las claves hayan sido dañadas;

e) los roles y responsabilidades para:

    1) la implementación de reglas para el uso efectivo de la criptografía;

    2) la gestión de claves, incluyendo la generación de claves (véase 8.24);

f) las normas que adoptar, así como los algoritmos criptográficos, la fortaleza del cifrado, las soluciones criptográficas y las prácticas de uso aprobadas o requeridas en la organización;

g) el impacto de usar información cifrada en controles que requieren inspección del contenido (por ejemplo, la detección del código dañino o el filtrado de contenidos).

Al implementar las reglas de la organización para el uso efectivo de la criptografía, se deberían tener en consideración las regulaciones y restricciones nacionales aplicables al uso de las técnicas criptográficas en las diferentes partes del mundo y las cuestiones sobre el flujo transfronterizo de información cifrada (véase 5.31).

Los contenidos de los acuerdos de nivel de servicio o los contratos con proveedores externos de servicios criptográficos (por ejemplo, con una autoridad de certificación) deberían cubrir las cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta en la prestación de los servicios (véase 5.22).

Gestión de claves

La gestión adecuada de claves requiere procesos seguros para la generación, almacenamiento, archivado, recuperación, distribución, retirada y destrucción de las claves criptográficas.

El sistema de gestión de claves debería estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) la generación de claves para diferentes sistemas criptográficos y para diferentes aplicaciones;

b) la emisión y obtención de certificados de clave pública;

c) la distribución de las claves a las entidades destinatarias, incluyendo como activarlas cuando se reciban;

d) el almacenamiento de las claves, incluyendo como los usuarios autorizados obtendrán acceso a éstas;

e) el cambio o la modificación de las claves, incluyendo reglas sobre cuando cambiarlas y cómo hacerlo;

f) el tratamiento de las claves comprometidas;

g) la revocación de las claves incluyendo como eliminarlas o desactivarlas (por ejemplo, cuando hayan sido comprometidas o cuando un usuario abandona la organización (en este caso, las claves deberían, también, archivarse);

h) la recuperación de claves perdidas o corruptas;

i) el respaldo o archivo de las claves;

j) la destrucción de claves;

k) el registro y la auditoría de las actividades relacionadas con la gestión de claves;

l) la configuración de las fechas de activación y desactivación de las claves de manera que éstas sólo puedan usarse durante el periodo de tiempo que fijen las reglas de la organización para la gestión de claves;

m) la gestión de las peticiones legales de acceso a claves criptográficas (por ejemplo, un proceso judicial puede requerir hacer disponible el acceso a la versión descifrada de información cifrada);

Todas las claves criptográficas deberían estar protegidas contra su modificación y pérdida. Adicionalmente, las claves secretas y privadas necesitan protección contra el uso no autorizado y contra su divulgación. El equipo utilizado para la generación, almacenamiento y archivo de claves debería estar protegido físicamente.

Además de la integridad de las claves públicas, debería considerarse también su autenticidad en muchos casos de uso.

Información adicional

La autenticidad de las claves públicas generalmente se aborda mediante procesos de gestión de éstas 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 un número pequeño de claves.

La criptografía se puede utilizar para lograr diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad: usando el cifrado de la información para proteger información sensible o crítica, ya sea almacenada o transmitida;

b) integridad o autenticidad: usando firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Usando los algoritmos con el fin de verificar la integridad de los archivos;

c) no-repudio: usando técnicas criptográficas para proporcionar pruebas de la ocurrencia o no de un evento o acción;

d) autenticación: usando técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso o que realizan transacciones con usuarios, entidades y recursos del sistema.

La serie de Normas ISO/IEC 11170 proporciona más información sobre la gestión de claves.

8.25 Seguridad en el ciclo de vida del desarrollo

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Proteger

Control

Se deberían establecer y aplicar reglas para el desarrollo seguro de aplicaciones y sistemas.

Propósito

Garantizar que la seguridad de la información se diseña e implementa dentro del ciclo de vida de desarrollo seguro de *software* y sistemas.

Orientación

El desarrollo seguro es un requisito en la construcción de un servicio, una arquitectura un *software* y un sistema. Para lograrlo se deberían considerar los siguientes aspectos:

a) la separación de los entornos de desarrollo, prueba y producción (véase 8.31);

b) las guías sobre la seguridad en el ciclo de vida de desarrollo de *software*:

   1) la seguridad en la metodología de desarrollo de *software* (véase 8.28 y 8.27);

   2) las guías de codificación segura para cada lenguaje de programación que se use (véase 8.28);

c) los requisitos de seguridad en la fase de especificación y diseño (véase 5.8);

d) los puntos de revisión de seguridad en proyectos (véase 5.8)

e) las pruebas de sistema y seguridad tales como pruebas de regresión, escaneo de código y pruebas de penetración (véase 8.29);

f) los repositorios seguros de código fuente y la configuración (véase 8.4 y 8.9);

g) la seguridad en el control de versiones (véase 8.32);

h) el conocimiento requerido en la seguridad de aplicaciones y la formación (véase 8.28);

i) la capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades (véase 8.28);

j) los requisitos de licencia y las alternativas para asegurar soluciones efectivas en coste evitando futuros problemas de licencia (véase 5.32).

Si se subcontrata el desarrollo, la organización debería asegurar que el proveedor cumple con las reglas de la organización para el desarrollo seguro (véase 8.30).

Información adicional

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 las aplicaciones

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Proteger

Control

Los requisitos de seguridad de la información deberían identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

Propósito

Garantizar que se identifican y abordan todos los requisitos de seguridad de información al desarrollar o adquirir aplicaciones.

Orientación

Los requisitos de seguridad de la aplicación deberían identificarse y especificarse. Estos requisitos se determinan, habitualmente, mediante una evaluación de riesgos. Los requisitos se deberían desarrollar con el apoyo de especialistas en seguridad de la información.

Los requisitos de seguridad de la información pueden cubrir un amplio rango de cuestiones, dependiendo del propósito de la aplicación.

Los requisitos de seguridad de aplicación deberían incluir, cuando sea aplicable:

a) el nivel de confianzas en la identidad de las entidades (por ejemplo, mediante la autenticación (véase 5.17, 8.2 y 8.5));

b) la identificación del tipo de información y su nivel de clasificación a ser procesado por la aplicación;

c) la necesidad de segregación de acceso y el nivel de acceso a datos y funciones en la aplicación;

d) la resiliencia contra ataques maliciosos o interrupciones no intencionadas (por ejemplo, la protección contra el desbordamiento de búfer o las inyecciones *SQL*);

e) los requisitos legales, estatutarios y reglamentarios en la jurisdicción en que la transacción se genere, trate, complete o almacene;

f) la necesidad de privacidad asociada a todas las partes involucradas;

g) los requisitos de protección de cualquier información confidencial;

h) la protección de los datos mientras se tratan, están en tránsito y en reposo;

i) la necesidad de cifrar de forma segura las comunicaciones entre todas las partes involucradas;

j) los controles de entrada, incluidas las verificaciones de integridad y la validación de entrada;

k) los controles automatizados (por ejemplo, límites de aprobación o aprobaciones duales);

l) los controles de salida, considerando también quién puede acceder a las salidas y su autorización;

m) las restricciones al contenido de los campos de "texto libre", ya que pueden conducir al almacenamiento no controlado de datos confidenciales (por ejemplo, datos personales);

n) los requisitos derivados del proceso de negocio, tales como registro y monitorización de transacciones o los requisitos de no repudio;

o) los requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces para registro y monitorización o los sistemas de detección de fuga de datos);

p) la gestión de los mensajes de error.

Servicios transaccionales

Además, para las aplicaciones que ofrecen servicios transaccionales entre la organización y otra parte, al identificar los requisitos de seguridad de la información se debería considerar lo siguiente:

a) el nivel de confianza que cada parte requiere en la identidad reclamada por la otra parte;

b) el nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para la identificación de la falta de integridad (por ejemplo, la verificación de redundancia cíclica, el *hashing*, las firmas digitales);

c) los procesos de autorización asociados a quien puede aprobar los contenidos, emitir o firmar documentos transaccionales clave;

d) la confidencialidad, la integridad, la prueba de envío y recepción de documentos clave y el 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) los requisitos sobre durante cuánto tiempo se debería mantener la confidencialidad de una transacción;

g) los seguros y otros requisitos contractuales.

Aplicaciones de pago y pedidos electrónicos

Además, cuando las aplicaciones involucren pedidos y pagos electrónicos, se debería considerar lo siguiente:

a) los requisitos para mantener la confidencialidad e integridad de la información del pedido;

b) el grado de verificación apropiado para verificar la información de pago proporcionada por el cliente;

c) evitar la pérdida o duplicar la información de la transacción;

d) el almacenamiento de los detalles de la transacción fuera de entornos de acceso público (por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización, y no ser retenida ni expuesta en medios de almacenamiento electrónico directamente accesibles desde Internet);

e) cuando se utiliza una autoridad de confianza (por ejemplo, para emitir y mantener firmas digitales o certificados digitales), la seguridad se integra e incorpora a lo largo de todo el proceso de gestión de certificados de extremo a extremo o del proceso de gestión de firma.

Algunas 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, véase 5.31 especialmente para la legislación criptográfica).

Información adicional

Las aplicaciones accesibles a través de las redes están sujetas a una variedad de amenazas relacionadas con la red, como por ejemplo actividades fraudulentas, disputas contractuales o divulgación de información al público; transmisión incompleta, enrutamiento erróneo, alteración no autorizada de mensajes, duplicación o repetición. Por lo tanto, son indispensables la evaluación detallada de riesgo y la determinación cuidadosa de los controles. Los controles requeridos incluyen, a menudo, métodos criptográficos para la autenticación y la transferencia segura de datos.

Se puede encontrar más información sobre la seguridad en las aplicaciones en la serie de Normas ISO/IEC 27034.

8.27 Arquitectura segura de sistemas y principios de ingeniería

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Proteger

Control

Los principios de ingeniería de sistemas seguros se deberían establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.

Propósito

Garantizar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida de desarrollo.

Orientación

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 (negocio, datos, aplicaciones y tecnología). La nueva tecnología debería analizarse en busca de riesgos de seguridad y el diseño debería revisarse con respecto a los patrones de ataque conocidos.

Los principios de ingeniería segura dan orientación sobre las técnicas de autenticación de usuarios, el control de sesiones seguro y la validación y sanitización de datos.

Los principios de ingeniería de sistemas seguros deberían incluir el análisis de:

a) la gama completa de controles de seguridad requerida 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) los controles de seguridad específicos requeridos por procesos de negocio particulares (por ejemplo, el cifrado de información sensible, la verificación de integridad y la firma digital de información);

d) dónde y cómo se aplicarán los controles de seguridad (por ejemplo, mediante la integración con la 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 consideración:

a) la necesidad de integrarse con una arquitectura de seguridad;

b) la infraestructura de seguridad técnica [por ejemplo, la infraestructura de clave pública (PKI), la gestión de identidad y acceso (IAM), la prevención de fuga de datos y la gestión de acceso dinámico];

c) la capacidad de la organización para desarrollar y mantener la tecnología elegida;

d) el coste, tiempo y complejidad de cumplir con los requisitos de seguridad;

e) las buenas prácticas actuales.

La ingeniería segura de sistemas debería implicar:

a) el uso de los principios de arquitectura de seguridad, tales como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación predeterminada", "fallo seguro", "desconfianza de los datos de entrada de aplicaciones externas", "seguridad en despliegue", "asumir incumplimiento", "privilegio mínimo", "facilidad de uso y capacidad de gestión" y "funcionalidad mínima";

b) la revisión del diseño orientada a la seguridad para ayudar a identificar las vulnerabilidades de seguridad de la información, asegurando que se especifican los controles de seguridad y se cumple con los requisitos de seguridad;

c) la documentación y reconocimiento formal de los controles de seguridad que no cumplan plenamente los requisitos (por ejemplo, debidos a requisitos de seguridad que los anulen);

d) el bastionado de los sistemas.

La organización debería considerar el principio de "confianza cero":

a) suponiendo que los sistemas de información de la organización ya han sido penetrados y, por lo tanto, no dependiendo tan solo de la seguridad del perímetro de la red;

b) empleando el enfoque de "nunca confiar y siempre verificar" para acceder a los sistemas de información;

c) garantizando que las solicitudes a los sistemas de información estén cifradas de extremo a extremo;

d) verificando cada solicitud a un sistema de información como si fuera originado en una red externa abierta, aunque estas solicitudes se originaran internamente en la organización (es decir, no confiando automáticamente en nada dentro o fuera del perímetro);

e) utilizando técnicas de "privilegio mínimo" y de control de acceso dinámico (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 final del usuario y clasificación de datos (véase 5.12);

f) autenticando siempre a los solicitantes y validando, siempre, 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 usuario (véase 5.16), los datos sobre el dispositivo final del usuario y la clasificación de datos (véase 5.12), por ejemplo, forzando la autenticación fuerte (por ejemplo, multifactorial, véase 8.5).

Los principios de ingeniería de seguridad establecidos deberían aplicarse, cuando corresponda, cuando se subcontrata el desarrollo 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 garantizar que las prácticas de ingeniería de seguridad de los proveedores se alineen con las necesidades de la organización.

Los principios de ingeniería de seguridad y los procedimientos establecidos de ingeniería deberían revisarse periódicamente para garantizar que contribuyan efectivamente a mejorar las normas de seguridad dentro del proceso de ingeniería. También deberían revisarse regularmente para garantizar que permanezcan actualizados para combatir cualquier nueva amenaza potencial y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Información adicional

Los principios de ingeniería segura se pueden aplicar al diseño o configuración de una variedad de técnicas, como:

- la tolerancia a fallos y otras técnicas de resiliencia;

- la segregación (por ejemplo, a través de virtualización o carga contenerizada);

- la resistencia a la manipulación.

Se pueden utilizar técnicas de virtualización seguras para evitar interferencias entre aplicaciones que se ejecutan en el mismo dispositivo físico. Si un atacante compromete 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 se pueden utilizar 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	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Proteger

Control

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 potenciales vulnerabilidades de seguridad de la información en el *software*.

Orientación

General

La organización debería establecer procesos para proporcionar una buena gobernanza para la programación segura. Se debería establecer y aplicar una línea de base segura mínima. Además, dichos procesos y gobernanza deberían extenderse y cubrir los componentes de *software* de terceros y el *software* de código abierto.

La organización debería monitorizar las amenazas del mundo real y actualizar el asesoramiento y la información sobre las vulnerabilidades del *software* para guiar los principios de programación segura de la organización a través de la mejora y el aprendizaje continuos. Esto puede ayudar a garantizar que se implementen prácticas de programación segura y efectivas para combatir el panorama de amenazas que cambia rápidamente.

Planificación y previo a la programación

Los principios de programación segura deberían usarse tanto en nuevos desarrollos como en escenarios de reutilización. Estos principios deberían aplicarse a las actividades de desarrollo tanto para los productos y servicios para la organización como para los que la organización proporcione a otros. La planificación y los requisitos previos antes de la programación deberían incluir:

a) las expectativas específicas de la organización y los principios aprobados para la programación segura que se utilizará para desarrollos de código internos y externos;

b) las prácticas comunes e históricas de programación y los defectos que condujeron a vulnerabilidades de seguridad de la información;

c) la configuración de las herramientas de desarrollo, como entornos de desarrollo integrados (IDE), para ayudar a la creación de código seguro;

d) el seguimiento de las guías proporcionadas por los proveedores de herramientas de desarrollo y entornos de ejecución, según corresponda;

e) el mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores);

f) la calificación de los desarrolladores para la escritura de código seguro;

g) el diseño y arquitectura seguros, incluido el modelado de amenazas;

h) las normas de programación seguras y, cuando corresponda, exigir su uso;

i) el uso de ambientes controlados para el desarrollo.

Durante la programación

Las consideraciones durante la programación deberían incluir:

a) las prácticas de programación seguras, específicas para los lenguajes y técnicas de programación que se utilizan;

b) la utilización de técnicas de programación seguras, como la programación en pares (cuando siempre hay dos personas trabajando en el código a la vez), la refactorización, la revisión por los pares, las iteraciones de seguridad y el desarrollo basado en pruebas;

c) la utilización de técnicas de programación estructurada;

d) la documentación del código y la eliminación de los defectos de programación, que puedan permitir la explotación de las vulnerabilidades de seguridad de la información;

e) prohibir el uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, partes 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) la superficie de ataque y el principio de privilegio mínimo;

b) un análisis de los errores de programación más comunes y documentar que estos han sido mitigados.

Revisión y mantenimiento

Una vez que el código se haya hecho operacional:

a) las actualizaciones deberían empaquetarse e implementarse de forma segura;

b) se deberían gestionar las vulnerabilidades de seguridad de la información reportadas (véase 8.8);

c) deberían registrarse los errores y los ataques que se sospechen y los registros deberían revisarse periódicamente para hacer los ajustes necesarios en el 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 proporcionan, típicamente, funciones como el control de acceso y el control de versiones).

Si utiliza herramientas y bibliotecas externas, la organización debería considerar:

a) garantizar que las bibliotecas externas se gestionan (por ejemplo, manteniendo un inventario de las bibliotecas utilizadas y sus versiones) y se actualizan regularmente de acuerdo con los ciclos de publicación;

b) la selección, autorización y reutilización de componentes bien revisados, 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 que proviene 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*, deberían considerarse lo siguiente:

a) el riesgo de que los controles incorporados y de procesos de integridad comprometidos;

b) si debiese obtenerse el consentimiento del vendedor;

c) la posibilidad de obtener los cambios necesarios del proveedor tales como actualizaciones estándar del programa;

d) el impacto en caso de que la organización se haga responsable del mantenimiento futuro del *software* como resultado de los cambios;

e) la compatibilidad con otro *software* en uso.

Información adicional

Un principio rector es garantizar que el código relevante para la seguridad se invoque cuando sea necesario y resista la manipulación. Los programas instalados a partir de código binario compilado 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 fuerte. Si el propietario de la aplicación puede acceder a los scripts mediante acceso remoto directo al servidor, también puede hacerlo un atacante. En tal caso, los servidores web deberían configurarse para evitar la exploración de directorios.

El código de la aplicación se diseña mejor asumiendo que siempre se está sujeto a ataques, por error o por acción maliciosa. Además, las aplicaciones críticas pueden diseñarse para ser tolerantes a fallos internos. 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, por ejemplo, una aplicación crítica financiera o de seguridad. El código que realiza las comprobaciones de los límites es simple y, por lo tanto, más fácil de probar que es correcto.

Algunas aplicaciones web son susceptibles a una variedad de vulnerabilidades introducidas por un diseño y una programación deficientes, como la inyección en bases de datos y los ataques de comandos en sitios cruzados. En estos ataques, las solicitudes pueden manipularse para abusar de la funcionalidad del servidor web.

En la serie de Normas ISO/IEC 15408 se puede encontrar más información sobre la evaluación de la seguridad de las TIC.

8.29 Pruebas de seguridad en desarrollo y aceptación

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_aplicaciones #Garantía_de_seguridad_de_la_información #Seguridad_de_sistemas_y_redes	#Proteger

Control

Deberían definirse e implementarse procesos de pruebas de seguridad en el ciclo de vida del desarrollo.

Propósito

Validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción.

Orientación

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 de acuerdo con un conjunto de requisitos que pueden expresarse como funcionales o no funcionales. Las pruebas de seguridad deberían incluir pruebas de:

a) funciones de seguridad [por ejemplo autenticación de usuarios (véase 8.5), restricción de acceso (véase 8.3) y uso de criptografía (véase 8.24)];

b) programación segura (véase 8.28);

c) configuraciones seguras (véase 8.9, 8.20 y 8.22) incluyendo sistemas operativos, cortafuegos 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) el cronograma detallado de actividades y pruebas;

b) las entradas y las salidas esperadas bajo un conjunto de condiciones;

c) los criterios para evaluar los resultados;

d) la decisión de realizar acciones adicionales si es 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 deberían realizarse pruebas de aceptación independientes para garantizar que el sistema funciona como se espera y tan solo como se espera (véase 5.8). Se debería considerar lo siguiente:

a) la realización de actividades de revisión de código como un elemento relevante para probar fallos de seguridad, incluyendo las entradas y condiciones no anticipadas;

b) la realización de un escaneo de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema;

c) la realización de pruebas de penetración para identificar código y diseño inseguros.

Para los componentes desarrollados externamente y para los comprados se debería seguir un proceso de adquisición. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados (véase 5.20). Antes de la adquisición, los productos y servicios deberían evaluarse según estos criterios.

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 son confiables (véase 8.31).

Información adicional

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 la monitorización de los entornos de prueba, las herramientas y las tecnologías para garantizar la eficacia de las pruebas. Las mismas consideraciones se aplican la monitorización de los sistemas de monitorización desplegados en entornos de desarrollo, prueba y producción. Para determinar cuántas capas de meta-test son útiles, se necesita analizar de acuerdo con la sensibilidad de los sistemas y de los datos.

8.30 Externalización del desarrollo

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Seguridad_de_sistemas_y_redes #Seguridad_de_aplicaciones #Seguridad_de_la_relación_con_los_proveedores	#Gobernanza_y_Ecosistema #Proteger

Control

La organización debería controlar, monitorizar y revisar las actividades relativas al desarrollo externalizado de sistemas.

Propósito

Garantizar que las medidas de seguridad de la información requeridas por la organización se implementan en el desarrollo de sistemas subcontratados.

Orientación

Cuando se subcontrata el desarrollo del sistema, la organización debería comunicar y acordar los requisitos y expectativas, y monitorizar 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) los acuerdos de licencia, de propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado (véase 5.32);

b) los requisitos contractuales para prácticas seguras de diseño, programación y pruebas (véase 8.25 a 8.29);

c) la provisión del modelo de amenazas a considerar por los desarrolladores externos;

d) las pruebas de aceptación para la calidad y exactitud de los entregables (véase 8.29);

e) la provisión de evidencias de que se han establecido niveles mínimos aceptables de seguridad y de privacidad (por ejemplo, informes de aseguramiento);

f) la provisión de evidencias de que se han realizado suficientes pruebas para proteger frente a la presencia de contenido malicioso (tanto intencionado como no intencionado) en el momento de la entrega;

g) la provisión de evidencias de que se han realizado pruebas suficientes para protegerse frente a la presencia de vulnerabilidades conocidas;

h) los acuerdos de depósito en garantía del código fuente (por ejemplo, por si el proveedor desaparece);

i) el derecho contractual a auditar los procesos de desarrollo y controles;

j) los requisitos de seguridad para el entorno de desarrollo (véase 8.31);

k) la toma en consideración de la legislación aplicable (por ejemplo, sobre protección de datos personales).

Información adicional

Se puede encontrar más información sobre las relaciones con los proveedores en la serie de Normas ISO/IEC 27036.

8.31 Separación de los entornos de desarrollo, prueba y producción

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Proteger

Control

Deberían separarse y protegerse los entornos de desarrollo, prueba y producción.

Propósito

Proteger el entorno de producción y los datos del compromiso debido a las actividades de desarrollo y prueba.

Orientación

Debería identificarse e implementarse el nivel necesario de separación entre los entornos de producción, prueba y desarrollo para evitar problemas en producción.

Se deberían considerar lo siguiente:

a) separar adecuadamente los sistemas de desarrollo y de 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* de desarrollo a producción;

c) probar los cambios a los sistemas y las aplicaciones en producción en un entorno de pruebas o de ensayo 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) los compiladores, editores y otras herramientas de desarrollo o programas de utilidad no deberían ser accesibles desde los sistemas de producción cuando no se requieran;

f) mostrar en los menús etiquetas identificando apropiadamente el entorno para reducir el riesgo de error;

g) no copiar información sensible en los entornos de desarrollo y prueba del sistema a menos que se proporcionen controles equivalentes en los sistemas de desarrollo y prueba.

En todos los casos, se deberían proteger los entornos de desarrollo y prueba teniendo en cuenta:

a) la aplicación de parches y la actualización de todas las herramientas de desarrollo, integración y prueba (incluidos *builders*, integradores, compiladores, sistemas de configuración y bibliotecas);

b) la configuración segura de sistemas y *software*;

c) control de acceso a los entornos;

d) la monitorización de los cambios a los entornos y al código almacenado en el mismo;

e) la monitorización segura de los entornos;

f) la realización de copias de seguridad de los entornos.

Una única persona no debería tener la posibilidad de realizar cambios tanto en desarrollo como en producción sin una revisión y aprobación previas. Esto se puede conseguir, por ejemplo, mediante la segregación de los derechos de acceso o mediante reglas monitorizadas. En situaciones excepcionales, se deberían implementar medidas adicionales como el registro detallado y la monitorización en tiempo real para detectar y actuar en caso de cambios no autorizados.

Información adicional

Sin medidas ni procedimientos adecuados, los desarrolladores y evaluadores que tienen acceso a los sistemas en producción pueden introducir riesgos significativos (por ejemplo, la modificación no deseada de archivos o del entorno del sistema, el fallo del sistema, la ejecución de código no autorizado ni probado en sistemas de producción, la divulgación de datos confidenciales, problemas de integridad de datos y 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 en conjunción con la implementación de requisitos de segregación de responsabilidades e implementando procesos de monitorización adecuados.

El personal de desarrollo y prueba también representa una amenaza a la confidencialidad de la información en producción. Las actividades de desarrollo y prueba pueden provocar cambios no deseados en el *software* o en la información si comparten el mismo entorno informático. Es deseable, por tanto., separar los entornos de desarrollo, prueba y producción para reducir el riesgo de cambio accidental o de acceso no autorizado al *software* de producción y a los datos de negocio (véase 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 el entorno de desarrollo o a través de implementaciones controladas para usuarios o servidores reales (por ejemplo, un pequeño grupo de usuarios piloto). En algunos casos, la prueba del producto puede realizarse mediante el uso del producto dentro de la organización. Además, para reducir el tiempo de inactividad de las implementaciones en vivo, se pueden tener dos entornos de producción idénticos donde solo uno está en vivo en un momento dado.

Son necesarios procesos de apoyo para el uso de datos de producción en entornos de desarrollo y prueba (véase 8.33).

Las organizaciones también pueden considerar la orientación proporcionada en esta sección en los entornos de formación para la capacitación del usuario final.

8.32 Gestión de cambios

Tipo de control	Propiedades de seguridad de información	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibiblidad	#Proteger	#Seguridad_de_las_aplicaciones #Seguridad_de_sistemas_y_redes	#Proteger

Control

Los cambios en las instalaciones de tratamiento 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.

Orientación

La introducción de nuevos sistemas y de cambios importantes en los sistemas existentes debería seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación gestionado. Para garantizar un control satisfactorio de todos los cambios, deberían existir responsabilidades y procedimientos de gestión.

Los procedimientos de control de cambios deberían documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de tratamiento de la información y en los sistemas de información, desde las primeras etapas de diseño, durante todo el ciclo de vida del desarrollo del sistema, y durante todos los esfuerzos de mantenimiento posteriores.

Siempre que sea factible, deberían integrarse los procedimientos de control de cambios para la infraestructura TIC y para el *software*.

Los procedimientos de control de cambios deberían incluir:

a) la planificación y evaluación del impacto potencial de los cambios considerando todas las dependencias;

b) la autorización de cambios;

c) la comunicación de los cambios a las partes interesadas pertinentes;

d) las pruebas y la aceptación de pruebas previa a los cambios (véase 8.29);

e) la implementación de cambios, incluidos los planes de implementación;

f) las consideraciones de emergencia y contingencia, incluidos los procedimientos de vuelta atrás;

g) el mantenimiento de registros de cambios que incluyan todo lo anterior;

h) la garantía de cambio de la documentación operativa (véase 5.37) y de los procedimientos del usuario cuando sea necesaria para que continúen siendo adecuados;

i) la garantía de modificación de los planes de continuidad de las TIC y de los procedimientos de respuesta y recuperación (véase 5.30) cuando sea necesario, para continúen siendo adecuados.

Información adicional

El control inadecuado de los cambios en las instalaciones de tratamiento de la información y en los sistemas de información es causa común de fallos del sistema o de fallos de seguridad. Los cambios en el entorno de producción, especialmente cuando se transfiere *software* del entorno de desarrollo al de operación, pueden afectar la integridad y disponibilidad de las aplicaciones.

Cambiar el *software* puede afectar el entorno de producción y viceversa.

Las buenas prácticas incluyen la prueba de los componentes de las TIC en un entorno segregado de los entornos de producción y de 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 a los cambios en aplicaciones e infraestructuras.

8.33 Datos de prueba

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad	#Proteger	#Protección_de_la_información	#Proteger

Control

Los datos de prueba se deberían seleccionar con cuidado y deberían ser protegidos y controlados.

Propósito

Garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas.

Orientación

La información de prueba debería seleccionarse para garantizar la confiabilidad en los resultados de las pruebas y la confidencialidad de la información operativa relevante. La información sensible (incluida la información personal identificable) no debería copiarse en los entornos de desarrollo y prueba (véase 8.31).

Se deberían aplicar las siguientes pautas para proteger las copias de la información operativa, cuándo se utilizan con fines de prueba, tanto si el entorno de prueba se construye internamente como si se hace 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 sensible 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 ésta.

La información de la prueba debería almacenarse de forma segura (para evitar la manipulación, que podría generar resultados no válidos) y solo debería usarse con fines de prueba.

Información adicional

Las pruebas del sistema y de aceptación pueden requerir volúmenes sustanciales de información de prueba que sean lo más parecida a la información operativa.

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes #Protección_de_la_información	#Gobernanza_Ecosistema #Proteger

Control

Las pruebas de auditoría y otras actividades de aseguramiento en la evaluación de los sistemas en producción deberían ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.

Propósito

Minimizar el impacto de la auditoría y otras actividades de aseguramiento sobre los sistemas operativos y sobre los procesos de negocio.

Orientación

Se observarán las siguientes pautas:

a) acordar las solicitudes de auditoría para el acceso a sistemas y a datos con una gestión adecuada;

b) acordar y controlar el alcance de las pruebas de auditoría técnica;

c) limitar las pruebas de auditoría al acceso de sólo lectura a *software* y datos. Si el acceso de sólo lectura no está disponible, para obtener la información necesaria un administrador experimentado que tenga los derechos de acceso necesarios ejecutará la prueba en nombre del auditor;

d) si se concede el acceso, se establecerán y verificarán los requisitos de seguridad (por ejemplo, antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (por ejemplo, portátiles o tabletas) antes de permitirles el acceso;

e) sólo se permitirá un acceso diferente al de sólo lectura a copias aisladas de los ficheros del sistema, suprimiéndolos cuando finalice la auditoría o, si existe obligación de mantener estos ficheros bajo los requisitos de documentación de auditoría, dándoles la protección adecuada;

f) identificar y acordar las solicitudes de procesamiento especial o adicional, como la ejecución de herramientas de auditoría;

g) ejecutar pruebas de auditoría que puedan afectar la disponibilidad del sistema fuera del horario de negocio;

h) monitorizar y registrar todos los accesos con fines de auditoría y prueba.

Información adicional

Las pruebas de auditoría y otras actividades de aseguramiento también pueden realizarse en los sistemas de desarrollo y prueba si estas pruebas pueden afectar, por ejemplo, la integridad del código o llevar a la divulgación de cualquier información sensible que resida en esos entornos.

Anexo A (Informativo)

Atributos de uso

A.1 Generalidades

Este anexo incluye una tabla para explicar el uso de los atributos como forma de crear distintas vistas de los controles. Los cinco ejemplos de atributos son (véase 4.2):

a) Tipos de control (#Preventivo, #Detectivo, #Correctivo)

b) Propiedades de la 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_los_recursos_humanos, #Seguridad_física, #Seguridad_del_Sistema_y_de_la_red, #Seguridad_de_las_ aplicaciones, #Configuración_segura, #Gestión_de_identidad_y_de_acceso, #Gestión_de_amenazas_y_vulnerabilidades, #Continuidad, #Seguridad_de_la_relación_con_ los_proveedores, #Cumplimiento_jurídico, #Gestión_de_eventos_de_seguridad_de_la_información, #Garantía_de_seguridad_de_la_información).

e) Ámbitos de seguridad (#Gobernanza_y_Ecosistema, #Protección, #Defensa, #Resiliencia)

La tabla A.1 contiene una lista de todos los controles de este documento con sus correspondientes valores de atributo.

Para filtrar u ordenar la lista se puede utilizar una herramienta como una simple hoja de cálculo o una base de datos, que puede incluir más información, como texto del control, orientaciones, orientaciones específicas de la organización o atributos (véase el capítulo A.2).

Tabla A.1 – Lista de controles y valores de los atributos

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
5.1	Políticas para la seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_ Ecosistema #Resiliencia
5.2	Roles y responsabilidades en seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_ Ecosistema #Resiliencia
5.3	Segregación de tareas	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernanza #Gestión de identidad y acceso	#Gobernanza_ Ecosistema #Resiliencia
5.4	Responsabilidades de la dirección	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_ Ecosistema #Resiliencia
5.5	Contacto con las autoridades	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resiliencia
5.6	Contacto con grupos de interés especial	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Responder	#Amenazas y vulnerabilidades de la dirección	#Defensa #Resiliencia
5.8	Seguridad de la información en la gestión de proyectos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gobernanza	#Gobernanza_ Ecosistema #Resiliencia
5.9	Inventario de información y otros activos asociados	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión de activos	#Gobernanza_ Ecosistema #Resiliencia
5.10	Uso aceptable de la información y activos asociados	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información	#Gobernanza_ Ecosistema #Resiliencia
5.11	Devolución de activos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos	#Protección
5.12	Clasificación de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Protección de la información	#Protección #Defensa
5.13	Etiquetado de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Protección de la información	#Protección #Defensa

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
5.14	Transferencia de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información	#Protección
5.15	Control de acceso	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad y gestión de acceso	#Protección
5.16	Gestión de identidad	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad y gestión de acceso	#Protección
5.17	Información de autenticación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad y gestión de acceso	#Protección
5.18	Derechos de acceso	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad y gestión de acceso	#Protección
5.19	Seguridad de la información en las relaciones con los proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con proveedores	#Gobernanza_ Ecosistema #Protección
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con proveedores	#Gobernanza_ Ecosistema #Protección
5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con proveedores	#Gobernanza_ Ecosistema #Protección
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad de las relaciones con proveedores #Garantías de seguridad de la información	#Gobernanza_ Ecosistema #Protección #Defensa
5.23	Seguridad de la información para el uso de servicios en la nube	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de las relaciones con proveedores	#Gobernanza_ Ecosistema #Protección
5.24	Planificación y preparación de la gestión de incidentes de seguridad de información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gobernanza #Gestión de eventos de seguridad de la información	#Defensa

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
5.25	Evaluación y decisión sobre los eventos de seguridad de información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#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
5.27	Aprender de los incidentes de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión de eventos de seguridad de la información	#Defensa
5.28	Recopilación de evidencias	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión de eventos de seguridad de la información	#Defensa
5.29	Seguridad de la información durante la interrupción	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Continuidad	#Protección #Resiliencia
5.30	Preparación para las TIC para la continuidad del negocio	#Correctivo	#Disponibilidad	#Responder	#Continuidad	#Resiliencia
5.31	Identificación de requisitos legales, reglamentarios y contractuales	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Legal y Compliance	#Gobernanza_ Ecosistema #Protección
5.32	Derechos de propiedad intelectual (DPI)	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Legal y Compliance	#Gobernanza_ Ecosistema
5.33	Protección de los registros	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Legal y Compliance #Gestión de activos #Protección de la información	#Defensa
5.34	Privacidad y protección de datos de carácter personal (DCP)	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Protección de la información #Legal y Compliance	#Protección
5.35	Revisión independiente de la seguridad de la información	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Garantías de seguridad de la información	#Gobernanza_ Ecosistema
5.36	Cumplimiento de las políticas y normas de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Legal y Compliance #Garantías de seguridad de la información	#Gobernanza_ Ecosistema

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
5.37	Documentación de procedimientos operacionales	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión de activos #Seguridad física #Sistema y seguridad de redes #Seguridad de las aplicaciones #Configuración segura #Gestión de identidad y de acceso #Gestión de amenazas y vulnerabilidades #Continuidad #Gestión de eventos de seguridad de la información	#Gobernanza_ Ecosistema #Protección #Defensa
6.1	Comprobación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos	#Gobernanza_ Ecosistema
6.2	Términos y condiciones de contratación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos	#Gobernanza_ Ecosistema
6.3	Concienciación, educación y formación en seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos	#Gobernanza_ Ecosistema
6.4	Proceso disciplinario	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad de los recursos humanos	#Gobernanza_ Ecosistema
6.5	Responsabilidad ante la finalización o cambio	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad de los recursos humanos #Gestión de activos	#Gobernanza_ Ecosistema
6.6	Acuerdos de confidencialidad o no divulgación	#Preventivo	#Confidencialidad	#Proteger	#Seguridad de los recursos humanos #Protección de la información #Relación con los proveedores	#Gobernanza_ Ecosistema
6.7	Teletrabajo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Protección de la información #Seguridad física #Sistema y seguridad de redes	#Protección

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
6.8	Notificación de los eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión de eventos de seguridad de la información	#Defensa
7.1	Perímetro de seguridad física	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.2	Controles físicos de entrada	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión de identidad y de acceso	#Protección
7.3	Seguridad de oficinas, despachos y recursos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión activos	#Protección
7.4	Monitorización de la seguridad física	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad física	#Protección #Defensa
7.5	Protección contra las amenazas físicas y ambientales	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.6	El trabajo en áreas seguras	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.7	Puesto de trabajo despejado y pantalla limpia	#Preventivo	#Confidencialidad	#Proteger	#Seguridad física	#Protección
7.8	Emplazamiento y protección de equipos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión activos	#Protección
7.9	Seguridad de los equipos fuera de las instalaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión activos	#Protección
7.10	Soportes de almacenamiento	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión activos	#Protección
7.11	Instalaciones de suministro	#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad física	#Protección
7.12	Seguridad del cableado	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física	#Protección
7.13	Mantenimiento de los equipos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad física #Gestión activos	#Protección #Resiliencia
7.14	Eliminación o reutilización segura de equipos	#Preventivo	#Confidencialidad	#Proteger	#Seguridad física #Gestión activos	#Protección

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
8.1	Dispositivos finales de usuario	#Preventivo	#Confidencialidad	#Proteger	#Gestión activos #Protección de la información	#Protección
8.2	Gestión de privilegios de acceso	#Preventivo	#Confidencialidad	#Proteger	#Gestión de identidad y de acceso	#Protección
8.3	Restricción del acceso a la información	#Preventivo	#Confidencialidad	#Proteger	#Gestión de identidad y de acceso	#Protección
8.4	Acceso al código fuente	#Preventivo	#Confidencialidad	#Proteger	#Gestión de identidad y de acceso #Seguridad de las aplicaciones #Configuración segura	#Protección
8.5	Autenticación segura	#Preventivo	#Confidencialidad	#Proteger	#Gestión de identidad y de acceso	#Protección
8.6	Gestión de capacidades	#Preventivo #Detectivo	#Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Continuidad	#Gobernanza_ Ecosistema
8.7	Controles contra el código malicioso	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Sistema y seguridad de 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_ Ecosistema #Protección #Defensa
8.9	Gestión de la configuración	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración segura	#Protección
8.10	Eliminación de la información	#Preventivo	#Confidencialidad	#Proteger	#Protección de la información #Legal y Compliance	#Protección
8.11	Enmascaramiento de datos	#Preventivo	#Confidencialidad	#Proteger	#Protección de la información	#Protección
8.12	Prevención de fugas de datos	#Preventivo #Detectivo	#Confidencialidad	#Proteger #Detectar	#Protección de la información	#Protección #Defensa
8.13	Copias de seguridad de la información	#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Defensa
8.14	Redundancia recursos de tratamiento de la información	#Preventivo	#Disponibilidad	#Proteger	#Continuidad #Gestión activos	#Protección #Resiliencia

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
8.15	Registros de eventos	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión de eventos de seguridad de la información	#Protección #Defensa
8.16	Seguimiento de actividades	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Gestión de eventos de seguridad de la información	#Defensa
8.17	Sincronización del reloj	#Detectivo #Correctivo	#Integridad	#Detectar #Responder	#Gestión de eventos de seguridad de la información	#Protección #Defensa
8.18	Uso de los programas de utilidad con privilegios	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema y seguridad de redes #Configuración segura #Aplicación de la seguridad	#Protección
8.19	Instalación del *software* en sistemas en producción	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración segura #Aplicación de la seguridad	#Protección
8.20	Seguridad de redes	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Sistema y seguridad de redes	#Protección
8.21	Seguridad de los servicios de red	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema y seguridad de redes	#Protección
8.22	Segregación en redes	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema y seguridad de redes	#Protección
8.23	Filtrado de webs	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema y seguridad de redes	#Protección
8.24	Uso de la criptografía	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración segura	#Protección
8.25	Seguridad en el ciclo de vida del desarrollo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Aplicación de la seguridad #Sistema y seguridad de redes	#Protección
8.26	Requisitos de seguridad de las aplicaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Aplicación de la seguridad #Sistema y seguridad de redes	#Protección #Defensa

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberse-guridad	Capacidades operativas	Dominios de seguridad
8.27	Arquitectura segura de sistemas y principios de ingeniería	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Aplicación de la seguridad #Sistema y seguridad de redes	#Protección
8.28	Codificación segura	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Aplicación de la seguridad #Sistema y seguridad de redes	#Protección
8.29	Pruebas de seguridad en desarrollo y aceptación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Aplicación de la seguridad #Gestión de eventos de seguridad de la información #Sistema y seguridad de redes	#Protección
8.30	Externalización del desarrollo	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Sistema y seguridad de redes #Aplicación de la seguridad #Relación con los proveedores	#Gobernanza_ Ecosistema #Protección
8.31	Separación de los entornos de desarrollo, prueba y producción	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Aplicación de la seguridad #Sistema y seguridad de redes	#Protección
8.32	Gestión de cambios	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Aplicación de la seguridad #Sistema y seguridad de redes	#Protección
8.33	Datos 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	#Sistema y seguridad de redes #Protección de la información	#Gobernanza_ 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 los controles #Correctivos

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.5	Contacto con las autoridades	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resiliencia
5.6	Contacto con grupos de interés especial	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Responder	#Amenazas y vulnerabilidades de la dirección	#Defensa #Resiliencia
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
5.26	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	Recopilación de evidencias	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión de eventos de seguridad de la 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
5.35	Revisión independiente de la seguridad de la información	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Garantías de seguridad de la información	#Gobernanza_ Ecosistema

ISO/IEC 27002 control identificador	Nombre de control	Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.37	Documentación de procedimientos operacionales	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión de activos #Seguridad física #Sistema y seguridad de redes #Seguridad de las aplicaciones #Configuración segura #Gestión de identidad y de acceso #Gestión de amenazas y vulnerabilidades #Continuidad #Gestión de eventos de seguridad de la información	#Gobernanza_Ecosistema #Protección #Defensa
6.4	Proceso disciplinario	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad de los recursos humanos	#Gobernanza_Ecosistema
8.7	Protección contra el código dañino	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Sistema y seguridad de redes #Protección de la información	#Protección #Defensa
8.13	Copia de seguridad	#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Defensa
8.16	Supervisión de actividades	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Gestión de eventos de seguridad de la información	#Defensa

A.2 Vistas organizativas

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 responder a 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 entender por qué es aconsejable un atributo específico de la organización. Por ejemplo, si una organización ha construido sus planes de tratamiento de riesgos [véase la Norma ISO/IEC 27001:2013, 6.1.3 e)] basándose en eventos, puede desear asociar un atributo de escenario de riesgo a cada control de este documento.

El beneficio de dicho atributo es agilizar 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 los que figuran en ISO/IEC 27001:2013, anexo A (que son emitidos en este documento) para garantizar que no se ha pasado por alto ningún control necesario.

Una vez conocidos el objetivo y los beneficios, el siguiente paso es determinar los valores de los atributos. Por ejemplo, la organización podría identificar 9 actos:

1) pérdida o robo del dispositivo móvil;
2) pérdida o robo en las instalaciones de la organización;
3) fuerza mayor, vandalismo y terrorismo;
4) fallo de *software*, *hardware*, electricidad, internet y comunicaciones;
5) fraude;
6) piratería informática;
7) divulgación;
8) infracción de la ley;
9) ingeniería social.

El segundo paso puede realizarse asignando identificadores a cada acto (por ejemplo, E1, E2, ..., E9).

El tercer paso consiste en copiar los identificadores y nombres de control de este documento en una hoja de cálculo o base de datos y asociar los valores de atributo a cada control, teniendo en cuenta que cada control puede tener más de un valor de atributo.

El último paso consiste en ordenar la hoja de cálculo o consultar la base de datos para extraer la información necesaria.

Otros ejemplos de atributos organizativos (y posibles valores) son:

a) madurez (valores de la serie de Normas ISO/IEC 33000 u otros modelos de madurez);
b) estado de implementación (por hacer, en curso, parcialmente implementado, totalmente implementado);
c) prioridad (1, 2, 3, etc.);
d) áreas organizativas implicadas (seguridad, TIC, recursos humanos, alta dirección, etc.);
e) acontecimientos;
f) activos implicados;
g) construir y ejecutar, para diferenciar los controles utilizados en las distintas etapas del ciclo de vida del servicio;
h) otros marcos con los que trabaja la organización o de los que puede estar en transición.

Anexo B (Informativo)

Correspondencia de ISO/IEC 27002:2022 (este documento) con ISO/IEC 27002:2013

El propósito de este anexo es proporcionar compatibilidad con versiones anteriores de la norma ISO/IEC 27002:2013 para organizaciones que actualmente utilizan esa norma 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 de este documento y los controles de ISO/IEC 27002:2013

Identificador de control ISO/IEC 27002:2022	Identificador de control ISO/IEC 27002:2013	Nombre de control
5.1	05.1.1, 05.1.2	Políticas para la seguridad de la información
5.2	06.1.1	Roles y responsabilidades en seguridad de la información
5.3	06.1.2	Segregación de tareas
5.4	07.2.1	Responsabilidades de gestión
5.5	06.1.3	Contacto con las autoridades
5.6	06.1.4	Contacto con grupos de interés 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 la información
5.14	13.2.1, 13.2.2, 13.2.3	Intercambio de información
5.15	09.1.1, 09.1.2	Control de acceso
5.16	09.2.1	Gestión de la identidad.
5.17	09.2.4, 09.3.1, 09.4.3	Información de 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 proveedores

Identificador de control ISO/IEC 27002:2022	Identificador de control ISO/IEC 27002:2013	Nombre de control
5.20	15.1.2	Requisitos de seguridad en contratos con terceros
5.21	15.1.3	Gestión de información de la información la cadena de suministro TIC
5.22	15.2.1, 15.2.2	Control revisión y gestión del cambio en la presentación del servicio de los proveedores
5.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
5.24	16.1.1	Planificación y preparación para la gestión de incidentes de seguridad
5.25	16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información
5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprendizaje de los incidentes de seguridad de la información
5.28	16.1.7	Recopilación de evidencias
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, estatuarios, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual (DPI)
5.33	18.1.3	Protección de los registros
5.34	18.1.4	Protección y privacidad de la PII
5.35	18.2.1	Revisión independiente de la seguridad de la información
5.36	18.2.2, 18.2.3	Conformidad con las políticas, reglas y estándares de seguridad de la información
5.37	12.1.1	Documentación de procedimientos operacionales
6.1	07.1.1	Investigación de antecedentes
6.2	07.1.2	Términos y condiciones del empleo
6.3	07.2.2	Conciencia, educación y capacitación en seguridad de la información
6.4	07.2.3	Proceso disciplinario
6.5	07.3.1	Responsabilidades ante la finalización o cambio
6.6	13.2.4	Acuerdos de confidencialidad o no revelación
6.7	06.2.2	Teletrabajo
6.8	16.1.2, 16.1.3	Notificación de eventos de seguridad de la información
7.1	11.1.1	Perímetro de seguridad física
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Seguridad de oficinas, despachos y recursos
7.4	Nuevo	Control de la seguridad física

Identificador de control ISO/IEC 27002:2022	Identificador de control ISO/IEC 27002:2013	Nombre de control
7.5	11.1.4	Protección contra las amenazas externas y ambientales
7.6	11.1.5	Trabajo en áreas seguras
7.7	11.2.9	Puesto de trabajo despejado y pantalla limpia
7.8	11.2.1	Emplazamiento y protección de equipos
7.9	11.2.6	Seguridad fuera de las instalaciones
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Soportes de almacenamiento
7.11	11.2.2	Instalaciones de suministro
7.12	11.2.3	Seguridad del cableado
7.13	11.2.4	Mantenimiento de los equipos
7.14	11.2.7	Reutilización o eliminación segura de equipos
8.1	06.2.1, 11.2.8	Dispositivos de punto final de los usuarios
8.2	09.2.3	Derechos de acceso privilegiados
8.3	09.4.1	Restricción del 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 capacidades
8.7	12.2.1	Protección contra el código dañino
8.8	12.6.1, 18.2.3	Gestión de las vulnerabilidades
8.9	Nuevo	Gestión de la configuración
8.10	Nuevo	Supresión de la información
8.11	Nuevo	Enmascaramiento de datos
8.12	Nuevo	Prevención de la fuga de datos
8.13	12.3.1	Copia de seguridad
8.14	17.2.1	Disponibilidad de los recursos de tratamiento de la información
8.15	12.4.1, 12.4.2, 12.4.3	Registro
8.16	Nuevo	Supervisión de actividades
8.17	12.4.4	Sincronización de relojes
8.18	09.4.4	Uso de programas de utilidad privilegiada
8.19	12.5.1, 12.6.2	Instalación de *software* en sistemas operativos
8.20	13.1.1	Seguridad de las redes
8.21	13.1.2	Seguridad de servicios de red
8.22	13.1.3	Segregación de redes
8.23	Nuevo	Filtrado web

Identificador de control ISO/IEC 27002:2022	Identificador de control ISO/IEC 27002:2013	Nombre de control
8.24	10.1.1, 10.1.2	Uso de la criptografía
8.25	14.2.1	Ciclo de vida de desarrollo seguro
8.26	14.1.2, 14.1.3	Requisitos de seguridad de las aplicaciones
8.27	14.2.5	Arquitectura de sistemas seguros y principios de ingeniería
8.28	Nuevo	Codificación segura
8.29	14.2.8, 14.2.9	Pruebas de seguridad en el desarrollo y la aceptación
8.30	14.2.7	Externalización del Desarrollo
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 sobre las pruebas
8.34	12.7.1	Protección de los sistemas de información durante la auditoría pruebas

La tabla B.2 proporciona la correspondencia de los controles especificados en la Norma ISO/IEC 27002:2013 con los de este documento.

Tabla B.2 – Correspondencia entre los controles de ISO/IEC 27002:2013 y los controles de este documento

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002:2022	Nombre de control de acuerdo con la Norma ISO/IEC 27002:2013
5		Políticas de seguridad de la información
5.1		Directrices de gestión de la seguridad de la información
5.1.1	5.1	Políticas para la seguridad de la información
5.1.2	5.1	Revisión de las políticas para la seguridad de la información
6		Organización de la seguridad de la información
6.1		Organización interna
6.1.1	5.2	Roles y responsabilidades en seguridad de la información
6.1.2	5.3	Segregación de tareas
6.1.3	5.5	Contacto con las 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		Los dispositivos móviles y el teletrabajo
6.2.1	8.1	Política de dispositivos móviles

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002:2022	Nombre de control de acuerdo con la Norma ISO/IEC 27002:2013
6.2.2	6.7	Teletrabajo
7		Seguridad relativa a los recursos humanos
7.1		Antes del empleo
7.1.1	6.1	Investigación de antecedentes
7.1.2	6.2	Términos y condiciones del empleo
7.2		Durante el empleo
7.2.1	5.4	Responsabilidades de gestión
7.2.2	6.3	Concienciación, educación y capacitación en seguridad de la información
7.2.3	6.4	Proceso disciplinario
7.3		Finalización del empleo o cambio en el puesto de trabajo
7.3.1	6.5	Responsabilidades ante la finalización o cambio
8		Gestión de activos
8.1		Responsabilidad sobre 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 la información
8.2.3	5.10	Manipulado de la información
8.3		Manipulación de los soportes
8.3.1	7.10	Gestión de soportes extraíbles
8.3.2	7.10	Eliminación de soportes
8.3.3	7.10	Soportes físicos en tránsito
9		Control de acceso
9.1		Requisitos de negocio para el control de acceso
9.1.1	5.15	Política de control de acceso
9.1.2	5.15	Acceso a las redes y a los servicios de red
9.2		Gestión de acceso de usuario
9.2.1	5.16	Registro y baja de usuario
9.2.2	5.18	Provisión de acceso de usuario
9.2.3	8.2	Gestión de privilegios de acceso

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002:2022	Nombre de control de acuerdo con la Norma ISO/IEC 27002:2013
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 usuario
9.2.6	5.18	Retirada o reasignación de los derechos de acceso
9.3		Responsabilidades del usuario
9.3.1	5.17	Uso de la información secreta de autenticación
9.4		Control de acceso a sistemas y aplicaciones
9.4.1	8.3	Restricción del 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 utilidades con privilegios del sistema
9.4.5	8.4	Control de acceso al código fuente de los programas
10		Criptografía
10.1		Controles criptográficos
10.1.1	8.24	Política de uso de los controles criptográficos
10.1.2	8.24	Gestión de claves
11		Seguridad física y del entorno
11.1		Áreas seguras
11.1.1	7.1	Perímetro de seguridad física
11.1.2	7.2	Controles físicos de entrada
11.1.3	7.3	Seguridad de oficinas, despachos y recursos
11.1.4	7.5	Protección contra las amenazas externas y ambientales
11.1.5	7.6	El trabajo en áreas seguras
11.1.6	7.2	Áreas de carga y descarga
11.2		Seguridad de los equipos
11.2.1	7.8	Emplazamiento y protección de equipos
11.2.2	7.11	Instalaciones de suministro
11.2.3	7.12	Seguridad del cableado
11.2.4	7.13	Mantenimiento de los equipos
11.2.5	7.10	Retirada de materiales propiedad de la empresa
11.2.6	7.9	Seguridad de los equipos fuera de las instalaciones
11.2.7	7.14	Reutilización o eliminación segura de equipos
11.2.8	8.1	Equipo de usuario desatendido
11.2.9	7.7	Política de puesto de trabajo despejado y pantalla limpia
12		Seguridad de las operaciones

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002:2022	Nombre de control de acuerdo con la Norma ISO/IEC 27002:2013
12.1		Procedimientos y responsabilidades operacionales
12.1.1	5.37	Documentación de procedimientos de los operación
12.1.2	8.32	Gestión de cambios
12.1.3	8.6	Gestión de capacidades
12.1.4	8.31	Separación de los recursos de desarrollo, prueba y operación
12.2		Protección contra el *software* malicioso (*malware*)
12.2.1	8.7	Controles contra el código malicioso
12.3		Copias de seguridad
12.3.1	8.13	Copias de seguridad de la información
12.4		Registros y supervisión
12.4.1	8.15	Registro de eventos
12.4.2	8.15	Protección de la información del registro
12.4.3	8.15	Registros de administración y operación
12.4.4	8.17	Sincronización del reloj
12.5		Control del *software* en explotación
12.5.1	8.19	Instalación del *software* en explotación
12.6		Gestión de la vulnerabilidad técnica
12.6.1	8.8	Gestión de las vulnerabilidades técnicas
12.6.2	8.19	Restricción en la instalación de *software*
12.7		Consideraciones sobre la auditoria de sistemas de información
12.7.1	8.34	Controles de auditoría de sistemas de información
13		Seguridad de las comunicaciones
13.1		Gestión de la seguridad de redes
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		Intercambio de información
13.2.1	5.14	Políticas y procedimientos de intercambio de información
13.2.2	5.14	Acuerdos de intercambio de información
13.2.3	5.14	Mensajería electrónica
13.2.4	6.6	Acuerdos de confidencialidad o no revelación
14		Adquisición, desarrollo y mantenimiento de los sistemas de información
14.1		Requisitos de seguridad en los sistemas de información

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002:2022	Nombre de control de acuerdo con la Norma ISO/IEC 27002:2013
14.1.1	5.8	Análisis de requisitos y especificaciones de seguridad de la información
14.1.2	8.26	Asegurar los servicios de aplicaciones en redes públicas
14.1.3	8.26	Protección de las transacciones de servicios de aplicaciones
14.2		Seguridad en el desarrollo y en los procesos de soporte
14.2.1	8.25	Política de desarrollo seguro
14.2.2	8.32	Procedimiento de control de cambios en sistemas
14.2.3	8.32	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
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	Externalización del desarrollo de *software*
14.2.8	8.29	Pruebas funcionales de seguridad de sistemas
14.2.9	8.29	Pruebas de aceptación de sistemas
14.3		Datos de prueba
14.3.1	8.33	Protección de los datos de prueba
15		Relación con proveedores
15.1		Seguridad en las relaciones con proveedores
15.1.1	5.19	Política de seguridad de la información en las relaciones con los proveedores
15.1.2	5.20	Requisitos de seguridad en contratos con terceros
15.1.3	5.21	Cadena de suministro de tecnología de la información y de las comunicaciones
15.2		Gestión de la provisión de servicios del proveedor
15.2.1	5.22	Control y revisión de la provisión de servicios del proveedor
15.2.2	5.22	Gestión de cambios en la provisión del servicio del proveedor
16		Gestión de incidentes de seguridad de la información
16.1		Gestión de incidentes de seguridad de la información y mejoras
16.1.1	5.24	Responsabilidades y procedimientos
16.1.2	6.8	Notificación de los eventos de seguridad de la información
16.1.3	6.8	Notificación de puntos débiles de la seguridad
16.1.4	5.25	Evaluación y decisión sobre los eventos de seguridad de información
16.1.5	5.26	Respuesta a incidentes de seguridad de la información
16.1.6	5.27	Aprendizaje de los incidentes de seguridad de la información

Identificador de control ISO/IEC 27002:2013	Identificador de control ISO/IEC 27002:2022	Nombre de control de acuerdo con la Norma ISO/IEC 27002:2013
16.1.7	5.28	Recopilación de evidencias
17		Aspectos de seguridad de la información para 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	Implementar la continuidad de la seguridad de la información
17.1.3	5.29	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
17.2		Redundancias
17.2.1	8.14	Disponibilidad de los recursos de tratamiento de la información
18		Cumplimiento
18.1		Cumplimiento de los requisitos legales y contractuales
18.1.1	5.31	Identificación de la legislación aplicable y de los requisitos contractuales
18.1.2	5.32	Derechos de propiedad intelectual (DPI)
18.1.3	5.33	Protección de los registros de la organización
18.1.4	5.34	Protección y privacidad de la información de carácter personal
18.1.5	5.31	Regulación de los controles criptográficos
18.2		Revisiones de la seguridad de la información
18.2.1	5.35	Revisión independiente de la seguridad de la información
18.2.2	5.36	Cumplimiento de las políticas y normas de seguridad
18.2.3	5.36, 8.8	Comprobación del cumplimiento técnico

Bibliografía

[1] ISO 9000, *Quality management systems. Fundamentals and vocabulary*.

[2] ISO 55001, *Asset management. Management systems. Requirements.*

[3] ISO/IEC 11770 (todas las partes), *Information security. Key management.*

[4] ISO/IEC 15408 (todas las partes), *Information technology. Security techniques. Evaluation criteria for IT security.*

[5] ISO 15489 (todas las partes), *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 (todas las partes), *Cloud computing. Service level agreement (SLA) framework*.

[9] ISO/IEC 19770 (todas las partes), *Information technology. IT asset management*.

[10] ISO/IEC 19941, *Information technology. Cloud computing. Interoperability and portability*.

[11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques.*

[12] ISO 21500, *Project, programme and portfolio management. Context and concepts*.

[13] ISO 21502, *Project, programme and portfolio management. Guidance on project management*.

[14] ISO 22301, *Security and resilience. Business continuity management systems. Requirements*.

[15] ISO 22313, *Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301*.

[16] ISO/TS 22317, *Societal security. Business continuity management systems. Guidelines for business impact analysis (BIA).*

[17] ISO 22396, *Security and resilience. Community resilience. Guidelines for information exchange between organizations*.

[18] ISO/IEC TS 23167, *Information technology. Cloud computing. Common technologies and techniques*.

[19] ISO/IEC 23751, *Information technology. Cloud computing and distributed platforms. Data sharing agreement (DSA) framework*.

[20] ISO/IEC 24760 (todas las partes), *IT Security and Privacy. A framework for identity management*.

[21] ISO/IEC 27001:2013, *Information technology. Security techniques. Information security management systems. Requirements*.

[22] ISO/IEC 27005, *Information technology. Security techniques. Information security risk management*.

[23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection. Guidelines for information security management systems auditing*.

[24] ISO/IEC TS 27008, *Information technology. Security techniques. Guidelines for the assessment of information security controls*.

[25] ISO/IEC 27011, *Information technology. Security techniques. Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[26] ISO/IEC TR 27016, *Information technology. Security techniques. Information security management. Organizational economics*.

[27] ISO/IEC 27017, *Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[28] ISO/IEC 27018, *Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.

[29] ISO/IEC 27019, *Information technology. Security techniques. Information security controls for the energy utility industry*.

[30] ISO/IEC 27031, *Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity*.

[31] ISO/IEC 27033 (todas las partes), *Information technology. Security techniques. Network security*.

[32] ISO/IEC 27034 (todas las partes), *Information technology. Application security*.

[33] ISO/IEC 27035 (todas las partes), *Information technology. Security techniques. Information security incident management*.

[34] ISO/IEC 27036 (todas las partes), *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 (todas las partes), *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 (todas las partes), *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

Para información relacionada con el desarrollo de las normas contacte con:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

Para información relacionada con la venta y distribución de las normas contacte con:

AENOR INTERNACIONAL S.A.U.
Tel.: 914 326 000
normas@aenor.com
www.aenor.com