ISO/IEC 27002:2022

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

Traducción propia exclusiva con fines académicos

ISO/IEC 27002:2022

SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD:

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Contenido

0. INTRODUCCIÓN 3

1. OBJETO Y CAMPO DE APLICACIÓN 4

2. REFERENCIAS NORMATIVAS 5

3. TERMINOS, DEFINICIONES Y ABREVIATURAS 5

4. ESTRUCTURA DE LA NORMA 9

5. CONTROLES ORGANIZACIONALES 11

6. CONTROLES DE PERSONAS 47

7. CONTROLES FÍSICOS ..... ¡Error! Marcador no definido.

8. CONTROLES TECNOLÓGICOS 65

ANEXO A: UTILIZACIÓN DE ATRIBUTOS 105

ANEXO B CORRESPONDENCIA DE LA ISO/IEC 27002:2022 CON LA ISO/IEC 27002:2013 105

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

INTERPRETACIÓN NORMA ISO/IEC 27002:2022

0. INTRODUCCIÓN

0.1. ANTECEDENTES Y CONTEXTO

Este documento está diseñado para que organizaciones de todos los tipos y tamaños lo utilicen:

- como referencia para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información (SI) en un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001;
- como documento de guía para determinar e implementar controles de SI comúnmente aceptados;
- para desarrollar directrices de gestión de la SI específicas de la industria y la organización, tomando en consideración sus entornos de riesgo de SI específicos.

0.2. REQUISITOS DE SI

Es fundamental que una organización determine sus requisitos de SI, para los que existen tres fuentes principales:

a) la evaluación de los riesgos para la organización, al tomar en consideración la estrategia y los PROPÓSITOS organizacionales. Esto se puede facilitar o apoyar mediante una evaluación de riesgos específica para la SI, lo que debería dar lugar a la determinación de los controles necesarios para garantizar que el riesgo residual para la organización cumple con sus criterios de aceptación de riesgos;

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

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

0.3. CONTROLES

Un control es una medida que modifica o mantiene el riesgo. Algunos de los controles de este documento son controles que modifican el riesgo, mientras que otros lo mantienen. Una política de SI, por ejemplo, solo puede mantener el riesgo, mientras que el cumplimiento de la política de SI puede modificar el riesgo. Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo. Este documento proporciona una mezcla genérica de controles de SI de la organización, las personas, la física y la tecnología derivados de prácticas recomendadas internacionalmente reconocidas.

0.4. DETERMINACIÓN DE LOS CONTROLES

La determinación de los controles depende de las decisiones de la organización tras una evaluación de riesgos en un ámbito claramente definido. Las decisiones relacionadas con los riesgos identificados se deberían basar en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque de gestión del riesgo aplicado. En la determinación de los controles también se deberían tener en cuenta todas las leyes y reglamentos nacionales e internacionales pertinentes. La determinación del control también depende de la manera en que los controles interactúan entre sí para proporcionar defensa en profundidad, y de las dependencias del contexto que se puedan presentar en determinado momento.

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

La organización también puede diseñar controles según sea necesario o identificarlos desde cualquier origen. Al especificar dichos controles, se debería considerar los recursos y la inversión necesarios para implementar y operar un control contra el valor organizacional obtenido. La ISO/IEC TR 27016 contiene orientación sobre las decisiones relativas a la inversión en un SGSI y las consecuencias económicas de estas decisiones en el contexto de requisitos de recursos que compiten entre sí.

Debería haber un equilibrio entre los recursos utilizados para implementar controles y el posible impacto 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 adecuadas, las prioridades para la gestión de los riesgos de SI y para la aplicación de los controles que se determinen necesarios para proteger contra estos riesgos.

Algunos de los controles de este documento se pueden considerar como principios rectores para la gestión de la SI y son aplicables a la mayoría de las organizaciones. En la ISO/IEC 27005 se puede encontrar más información sobre la determinación de controles y otras opciones de tratamiento de riesgos.

0.5. ELABORACIÓN DE DIRECTRICES ESPECÍFICAS DE LA ORGANIZACIÓN

Este documento es un punto de partida para elaborar directrices específicas para cada organización. No todos los controles y directrices de este documento se pueden aplicar a todas las organizaciones. También se pueden requerir controles y directrices adicionales que no están incluidos para abordar las necesidades específicas de la organización y los riesgos que se han identificado. Cuando se desarrollan documentos que contienen directrices o controles adicionales, puede ser útil incluir referencias cruzadas a cláusulas en este documento para futuras referencias.

0.6. CONSIDERACIONES SOBRE EL CICLO DE VIDA

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

Asimismo, los sistemas de información y otros activos relevantes para la SI tienen ciclos de vida dentro de los cuales se conciben, especifican, diseñan, desarrollan, prueban, implementan, usan, mantienen y eventualmente se retiran del servicio y eliminan. La SI se debería considerar en cada etapa. Los nuevos proyectos de desarrollo de sistemas y los cambios en los sistemas existentes ofrecen oportunidades para mejorar los controles de seguridad, tomando en consideración los riesgos y las lecciones aprendidas de los incidentes por parte de la organización.

0.7. NORMAS INTERNACIONALES RELACIONADAS

Aunque esta norma ofrece guía sobre una amplia gama de controles de SI que se aplican comúnmente en muchas organizaciones, otros documentos de la familia ISO/IEC 27000 proporcionan orientación o requisitos complementarios sobre otros aspectos del proceso general de gestión de la SI.

La norma ISO/IEC 27000 provee una introducción general a los SGSI y a la familia de documentos. La ISO/IEC 27000 proporciona un glosario que define la mayoría de los términos utilizados en la familia de documentos ISO/IEC 27000 y describe el alcance y los propósitos de cada miembro de la familia.

1. OBJETO Y CAMPO DE APLICACIÓN

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

Este documento proporciona un conjunto de controles genéricos de SI de referencia, incluida la guía de implementación, y está diseñado para que lo utilicen las organizaciones:

a) en el contexto de un SGSI basado en ISO/IEC 27001;

b) para implementar controles de SI basados en prácticas internacionalmente reconocidas;

c) para desarrollar directrices de gestión de la SI específicas de la organización.

2. REFERENCIAS NORMATIVAS

No hay referencias a otras normas.

3. TERMINOS, DEFINICIONES Y ABREVIATURAS

3.1. TERMINOS Y DEFINICIONES

La ISO y la IEC mantienen bases de datos de términos y definiciones para su uso en la normalización en las siguientes direcciones:

- ISO Plataforma de navegación en línea: https://www.iso.org/obp

- IEC Electropedia: https://www.electropedia.org/

3.1.1 Control de acceso (access control). Medios para garantizar que el acceso físico y lógico a los activos (3.1.2) esté autorizado y restringido en función de los requisitos organizacionales y de la SI.

3.1.2 Activo (*asset*). Cualquier cosa o entidad que tenga valor para la organización.

Nota 1: En el contexto de la SI, se pueden distinguir dos tipos de activos:

- los activos principales:
  - información;
  - procesos y actividades organizacionales (3.1.27);
- los activos de apoyo (de los que dependen los activos primarios) de todos los tipos, por ejemplo:
  - hardware;
  - software;
  - red;
  - personal (3.1.20);
  - sitio;
  - estructura de la organización.

3.1.3 Ataque (*attack*). Intento no autorizado exitoso o fallido de destruir, alterar, desactivar y obtener acceso a un activo (3.1.2) o cualquier intento de exponer, robar o hacer uso no autorizado de un activo (3.1.2).

3.1.4 Autenticación (*authentication*). Garantía de que una característica de una entidad (3.1.11) es correcta.

3.1.5 Autenticidad (*authenticity*). Propiedad de que una entidad (3.1.11) es lo que dice ser.

3.1.6 Cadena de custodia (*chain of custody*). Posesión, movimiento, manipulación y ubicación

demostrables del material desde un punto a otro en el tiempo.

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

3.1.7 Información confidencial (confidential information). Información que no se pretende poner a disposición o divulgar a personas o entidades (3.1.11) o procesos no autorizados (3.1.27).

3.1.8 Control (control). Medida que mantiene o modifica el riesgo.

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

Nota 2: Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto.

3.1.9 Interrupción (disruption). Incidente ya sea anticipado o imprevisto, que causa una desviación negativa y no planificada de la entrega prevista de productos y servicios según los propósitos organizacionales.

3.1.10 Dispositivo final (*endpoint device*). Dispositivo de hardware de tecnología de la información y las comunicaciones (TIC) conectado a la red.

Nota 1: El dispositivo de punto final puede ser un computador de mesa, portátil, smartphone, tablet, impresora u otro hardware especializado, incluidos medidores inteligentes y dispositivos de Internet de las cosas (IoT).

3.1.11 Entidad (entity). Elemento pertinente para el funcionamiento de un dominio que tiene una existencia reconociblemente distinta.

Nota 1: Una entidad puede ser física o lógica. Por ejemplo: una persona, una organización, un dispositivo, un grupo de dichos elementos, un abonado humano a un servicio de telecomunicaciones, una tarjeta SIM, un pasaporte, una tarjeta de interfaz de red, una aplicación de software, un servicio o un sitio web.

3.1.12 Servicio de procesamiento de información (information processing facility). Cualquier sistema de procesamiento de información, servicio o infraestructura o la ubicación física que lo aloja.

3.1.13 Violación de la SI (*information security breach*). Compromiso de la SI que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a, información protegida transmitida, almacenada o procesada de otro modo.

3.1.14 Evento de SI (*information security event*). Incidente que indica una posible afectación a la SI (3.1.13) o una falla de los controles (3.1.8).

3.1.15 Incidente de SI (*information security incidente*). Uno o varios eventos de SI relacionados e identificados (3.1.14) que pueden dañar los activos (3.1.2) de una organización o poner en peligro sus operaciones.

3.1.16 Gestión de incidentes de SI (*information security incident management*). Ejecución de un enfoque coherente y eficaz para el tratamiento de los incidentes de SI (3.1.15).

3.1.17 Sistema de información (*information system*). Conjunto de aplicaciones, servicios, activos de tecnología de la información (3.1.2) u otros componentes de tratamiento de la información.

3.1.18 Parte interesada (*interested party*). Persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad.

3.1.19 No repudio (*non-repudiation*). Capacidad para probar la ocurrencia de un evento o acción reclamada y sus entidades de origen (3.1.11).

3.1.20 Personal (*personnel*). Personas que trabajan bajo la dirección de la organización.

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

3.1.21 Información de identificación personal (IIP- personally identifiable information, PII). Cualquier información que (a) se pueda utilizar para establecer un vínculo entre la información y la persona natural a la que se refiere dicha información, o (b) esté o pueda estar directa o indirectamente vinculada a una persona natural.

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

3.1.22 Titular de la IIP (PII principal). Persona natural a la que se refiere la información de identificación personal (IIP) (3.1.21).

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

3.1.23 Procesador de IIP (PII processor). Parte interesada en la privacidad que procesa IIP (3.1.21) en nombre y de acuerdo con las instrucciones de un controlador de IIP.

3.1.24 Política (*policy*). Intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

3.1.25 Evaluación del impacto en la privacidad EIP (*privacy impact assessment* PIA). Proceso global (3.1.27) de identificar, analizar, evaluar, consultar, comunicar y planificar el tratamiento de posibles impactos en la privacidad con respecto al procesamiento de información de identificación personal (IIP) (3.1.21), enmarcado dentro del marco más amplio de gestión de riesgos de una organización.

3.1.26 Procedimiento (*procedure*). Forma específica de llevar a cabo una actividad o un proceso (3.1.27).

3.1.27 Proceso (*process*). Conjunto de actividades interrelacionadas que utiliza o transforma entradas para proporcionar un resultado.

3.1.28 Registro (*record*). Información que se crea, recibe y mantiene como prueba y como activo (3.1.2) por parte de una organización o persona, en cumplimiento de sus obligaciones legales o en la transacción de un negocio.

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

3.1.29 Punto objetivo de recuperación POR (recovery point objective, RPO). Punto en el tiempo en el que se recuperarán los datos después de que se haya producido una interrupción (3.1.9).

3.1.30 Tiempo objetivo de recuperación TOR (*recovery time objective* RTO). Período de tiempo dentro del cual los niveles mínimos de servicios o productos y los sistemas, aplicaciones o funciones de apoyo se deberían recuperar después de una interrupción (3.1.9).

3.1.31 Confiabilidad (*reliability*). Propiedad del comportamiento y resultados previstos coherentes.

3.1.32 Regla (*rule*). Principio aceptado o instrucción que indique las expectativas de la organización sobre lo que se requiere hacer, lo que se permite o no se permite.

Nota 1: Las normas se pueden expresar formalmente en políticas específicas por temas (3.1.35) y en otros tipos de documentos.

3.1.33 Información sensible (sensitive information). Información que se debería proteger de la indisponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en una persona organización, seguridad nacional o seguridad pública.

3.1.34 Amenaza (*threat*). Causa potencial de un incidente no deseado, que puede provocar daños en un sistema u organización.

3.1.35 Política específica por tema (*topic-specific policy*). Intenciones y guía sobre un asunto o tema específico, expresadas formalmente por el nivel apropiado de gestión.

Nota 1: Las políticas específicas pueden expresar formalmente reglas (3.1.32) o normas organizacionales.

Nota 2: Algunas organizaciones utilizan otros términos para estas políticas específicas.

Nota 3: Las políticas específicas a las que se hace referencia en este documento están relacionadas con la SI. Por ejemplo: directiva específica sobre control de acceso (3.1.1), directiva específica sobre escritorio y pantalla limpia.

3.1.36 Usuario (user). Parte interesada (3.1.18) con acceso a los sistemas de información de la organización (3.1.17). **Por e**jemplo: Personal (3.1.20), clientes, proveedores.

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

Nota 1: El dispositivo final de usuario se puede referir a computadores de mesa, portátiles, smartphones, tabletas, etc.

3.1.38 Vulnerabilidad (vulnerability). Debilidad de un activo (3.1.2) o control (3.1.8) que puede ser explotado por una o más amenazas (3.1.34).

3.2. ABREVIATURAS

ABAC	control de acceso basado en atributos.
ACL	lista de control de acceso.
BIA	análisis de impacto de negocio.
BYOD	traiga su propio dispositivo.
CAPTCHA	prueba de Turing pública y automática para diferenciar máquinas y humanos.
CPU	unidad central de procesamiento.
DAC	control de acceso discrecional.
DNS	sistema de nombres de dominio.
GPS	sistema de posicionamiento global.
IAM	gestión de identidades y accesos.
ICT	tecnologías de la información y la comunicación.
ID	identificador.
IDE	entorno de desarrollo integrado.
IDS	sistema de detección de intrusiones.
IoT	internet de las cosas.
IP	protocolo de internet.
IPS	sistema de prevención de intrusiones.
IT	tecnología de la información
ISMS	sistema de gestión de la SI

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

MAC	control de acceso obligatorio
NTP	protocolo de tiempo de red
PIA	evaluación del impacto en la privacidad
PII	información de identificación personal
P/N	número de identificación personal
PKI	infraestructura de clave pública
PTP	protocolo de tiempo de precisión
RBAC	control de acceso basado en roles
RPO	punto objetivo de recuperación
RTO	tiempo objetivo de recuperación
SAST	pruebas de seguridad de aplicaciones estáticas
SD	tarjeta de memoria
SDN	redes definidas por software
SD-WAN	red de área extensa definida por software
SIEM	información de seguridad y gestión de eventos
SMS	servicio de mensajes cortos
SQL	lenguaje de consulta estructurado
SSO	inicio de sesión único
SWID	identificación del software
UEBA	análisis de comportamiento de usuarios y entidades
UPS	sistema de alimentación ininterrumpida
URL	localizador uniforme de recursos
USB	bus serial universal
VM	máquina virtual
VPN	red privada virtual
WiFi	fidelidad inalámbrica

4. ESTRUCTURA DE LA NORMA

4.1. CLÁUSULAS

Las cláusulas se estructuran de la siguiente manera:

a) Controles organizacionales (Cláusula 5).
b) Controles de las personas (Cláusula 6).
c) Controles físicos (Cláusula 7).
d) Controles tecnológicos (Cláusula 8).
e) Anexo A - Uso de los atributos. Explica cómo la organización puede utilizar atributos (ver 4.2) para crear sus propias vistas basándose en los atributos de control definidos en este documento o en su propia creación.
f) Anexo B – Correspondencia con la ISO/IEC 27002:2013.

4.2. TEMAS Y ATRIBUTOS

La categorización de los controles de las cláusulas 5 a la 8 se denomina temas. Los controles se clasifican como:

a) personas, si se refieren a personas individuales;

b) físicos, si se refieren a objetos físicos;

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

c) tecnológico, si se refiere a la tecnología;

d) de lo contrario, se categorizan como organizacionales.

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

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

a) **Tipo de control:** atributo para ver los controles desde la perspectiva de cuándo y cómo modifica el control el riesgo con respecto a la ocurrencia de un incidente de SI. Los valores son **Preventivo** (para evitar que se produzca un incidente de SI), de **Detectivo** (para detectar si se produce un incidente de SI) y **Correctivo** (para actuar después de que se produzca un incidente de SI).

b) **Propiedades de SI:** atributo que establece qué característica de la información contribuirá a conservar el control. Los valores de atributo consisten en **Confidencialidad**, **Integridad** y **Disponibilidad**.

c) **Conceptos de ciberseguridad:** atributo para ver los controles desde la perspectiva de la asociación de los controles a los conceptos de ciberseguridad definidos en el marco de ciberseguridad de la norma ISO/IEC TS 27110. Los valores son **Identificar**, **Proteger**, **Detectar**, **Responder** y **Recuperar**.

d) **Capacidades operativas:** atributo para ver los controles desde la perspectiva de las capacidades del profesional SI que los opera. Los valores son: **Gobierno**, **Gestión de activos**, **Protección de información**, **Seguridad de recursos humanos**, **Seguridad física**, **Seguridad del sistema y de la red**, **Seguridad aplicación**, **Configuración segura**, **Gestión de acceso e identidad**, **Gestión de amenazas y vulnerabilidades**, **Continuidad**, **Seguridad de las relaciones con los proveedores**, **Conformidad jurídica**, **Gestión de eventos de la información** y **Aseguramiento de la información**.

e) **Dominios de seguridad:** atributo para ver los controles desde la perspectiva de cuatro dominios de SI: "**Gobierno y ecosistema**", que incluye "Gobierno y gestión de riesgos de seguridad de sistemas de información" y "Gestión de ecosistema de ciberseguridad" (incluidas las partes interesadas internas y externas); "**Protección**" que incluye "Arquitectura de seguridad de TI", "Administración de seguridad de TI", "Gestión de identidades y acceso", "Mantenimiento de seguridad de TI" y "Seguridad física y ambiental"; "**Defensa**" que incluye "Detección" y "Gestión de incidentes de seguridad informática"; "**Resiliencia**" que incluye la "continuidad de las operaciones" y la "gestión de crisis". Los valores de los atributos consisten en **Gobierno y Ecosistema**, **Protección**, **Defensa** y **Resiliencia**.

Los atributos se consideran suficientemente genéricos para que los utilicen distintos tipos de organizaciones. Éstas pueden optar por ignorar uno o varios de los atributos. También pueden crear atributos propios (con los valores de atributo correspondientes) para crear sus propias vistas organizativas. La cláusula A.2 incluye ejemplos de tales atributos.

4.3. DISEÑO DEL CONTROL

El diseño de cada control contiene:

- **Nombre del control:** Nombre corto del control.

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

- **Tabla de atributos:** Tabla que muestra los valores de cada atributo para el control. A esta tabla se ha agregado la identificación del(de los) Control(es) de la ISO/IEC 27001:2013 correspondientes.
- **Control:** La descripción del control.
- **Propósito:** Por qué debería implementarse el control.
- **Orientación:** Cómo debería implementarse el control.
- **Otra información:** texto adicional explicativo o referencias a otros documentos relacionados.

En algunos casos se usan subtítulos subrayados en el texto de la orientación para hacerlos más legibles en los casos en que la orientación es larga y aborda múltiples tópicos.

5. CONTROLES ORGANIZACIONALES

5.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013[1]
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobierno	#Gobierno_y_ecosistema #Resiliencia	5.1.1 5.1.2
CONTROL	La política de SI y las políticas de temas específicos deberían ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal y las partes interesadas pertinentes y revisadas a intervalos planificados y si se producen cambios significativos.					
PROPÓSITO	Garantizar la idoneidad, adecuación y eficacia continuas de la dirección y el apoyo a la SI de acuerdo con los requisitos organizacionales, legales, reglamentarios y contractuales.					
ORIENTACIÓN	En el nivel más alto, la organización debería definir una “política de SI” que sea aprobada por la alta dirección y que establezca el enfoque de la organización para administrar su SI. La política de SI debería tener en cuenta los requisitos derivados de: a) estrategia y requisitos organizacionales; b) reglamentos, legislación y contratos; c) los riesgos y amenazas actuales y proyectados para la SI. La política de SI debería contener declaraciones relativas a: a) definición de la SI; b) objetivos de SI o el marco para establecerlos; c) principios que orienten todas las actividades relacionadas con la SI; d) compromiso de satisfacer los requisitos aplicables relacionados con la SI; e) compromiso con la mejora continua del SGSI; f) asignación de responsabilidades para la gestión de la SI a funciones definidas; g) procedimientos para manejar exenciones y excepciones. La administración superior debería aprobar cualquier cambio en la política de SI. En un nivel inferior, la política de SI debiera apoyarse en políticas específicas según sea necesario, a fin de seguir asignando la aplicación de los controles de SI. Las políticas específicas de un tema se estructuran normalmente para satisfacer las necesidades de determinados grupos de destino dentro de una organización o para cubrir determinadas áreas de seguridad. Las políticas específicas de cada tema deberían estar alineadas y complementarse con la política de SI de la organización. Algunos ejemplos de temas incluyen: a) control de acceso; b) seguridad física y ambiental; c) gestión de activos; d) transferencia de información; e) configuración y gestión seguras de dispositivos finales de usuario; f) seguridad de red;					

[1] Atributo agregado por SGS para facilitar la comprensión de los cambios respecto a la versión 2013 de la norma.

<table>
<tr><td></td><td>g) gestión de incidentes de SI;
h) respaldos;
i) criptografía y gestión de claves;
j) clasificación y tratamiento de la información;
k) gestión de las vulnerabilidades técnicas;
l) desarrollo seguro.
La responsabilidad de la elaboración, revisión y aprobación de las políticas específicas del tema se debería asignar al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica. La revisión debería incluir la evaluación de las oportunidades de mejora de la política de SI de la organización y de las políticas de temas específicos y la gestión de la SI en respuesta a los cambios en:
a) la estrategia organizacional de la organización;
b) el entorno técnico de la organización;
c) reglamentos, estatutos, legislación y contratos;
d) riesgos de SI;
e) el entorno actual y proyectado de amenazas a la SI;
f) lecciones aprendidas de incidentes y eventos de SI.
La revisión de la política de SI y de las políticas específicas de cada tema debería tener en cuenta los resultados de las revisiones y auditorías. Se debería considerar la revisión y actualización de otras políticas relacionadas cuando se cambia una política con la finalidad de mantener la coherencia.
La política de SI y las políticas específicas de cada tema se deberían comunicar al personal pertinente y a las partes interesadas de una forma que sea pertinente, accesible y comprensible para el lector al que se dirige. Los destinatarios de las políticas deberían estar obligados a reconocer que comprenden y aceptan cumplir con las políticas cuando sea aplicable. La organización puede determinar los formatos y nombres de estos documentos normativos que satisfagan las necesidades de la organización. En algunas organizaciones, la directiva de SI y las políticas específicas pueden estar en un solo documento. La organización puede nombrar estas políticas específicas como estándares, directivas, lineamientos u otras formas.
Si la política de SI o cualquier política específica de un tema se distribuye fuera de la organización, se debería tener cuidado de no revelar información confidencial de forma incorrecta.
La tabla siguiente muestran las diferencias entre la política de SI y la política específica de un tema.
<table>
<tr><th></th><th>Política de SI</th><th>Política específica por tema</th></tr>
<tr><td>Nivel de detalle</td><td>General o de alto nivel</td><td>Específico y detallado</td></tr>
<tr><td>Documentado y aprobado formalmente por</td><td>Alta dirección</td><td>Nivel apropiado de gestión</td></tr>
</table>
</td></tr>
<tr><td>OTRA INFORMACIÓN</td><td>Las políticas específicas de cada tema pueden variar según las organizaciones.</td></tr>
</table>

5.2. FUNCIONES Y RESPONSABILIDADES EN MATERIA DE SI

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Gobierno**	**#Gobierno_y_ecosistema #Protección #Resiliencia**	**6.1.1**
CONTROL	Las funciones y responsabilidades de SI se deberían definir y asignar de acuerdo con las necesidades de la organización.					
PROPÓSITO	Establecer una estructura definida, aprobada y entendida para la implementación operación y gestión de la SI dentro de la organización.					
ORIENTACIÓN	La asignación de las funciones y responsabilidades de SI se debería realizar de acuerdo con la política de SI y las políticas específicas de cada tema (ver 5.1). La organización debería definir y gestionar las responsabilidades de: a) protección de la información y otros activos asociados; b) ejecución de procesos específicos de SI;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	c) actividades de gestión de riesgos de SI y, en particular, aceptación de riesgos residuales (por ejemplo, para los propietarios de riesgos); d) todo el personal que utilice la información y otros activos asociados. Estas responsabilidades se deberían complementar, cuando sea necesario, con una guía más detallada para sitios e instalaciones de procesamiento de información específicos. Las personas con responsabilidades asignadas en materia de SI pueden asignar tareas de seguridad a otras personas. Sin embargo, siguen siendo responsables y deberían determinar que cualquier tarea delegada se ha realizado correctamente. Se debería definir, documentar y comunicar cada área de seguridad de la que son responsables los individuos. Se deberían definir y documentar los niveles de autorización. Las personas que asumen una función específica de SI deberían ser competentes en cuanto a los conocimientos y habilidades requeridos por la función y deberían recibir apoyo para mantenerse al día con los desarrollos relacionados con la función y requeridos para cumplir con las responsabilidades de esta.
OTRA INFORMACIÓN	Muchas organizaciones nombran a un administrador de SI para que asuma la responsabilidad general del desarrollo e implementación de la SI y para que apoye la identificación de riesgos y los controles mitigantes. Sin embargo, la responsabilidad de la obtención de recursos y la aplicación de los controles a menudo recae en los directores individuales. Una práctica común es nombrar un propietario para cada activo que se haga responsable de su protección diaria. En función del tamaño y la obtención de recursos de una organización, la SI puede estar cubierta por funciones o tareas dedicadas que se llevan a cabo además de las funciones existentes.

5.3. SEGREGACIÓN DE FUNCIONES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gobierno #Gestion_de_la_identidad_y_del_acceso**	**#Gobierno_y_ecosistema**	**6.1.2**
CONTROL	Las funciones y las áreas de responsabilidad conflictivas deberían estar separadas.					
PROPÓSITO	Reducir el riesgo de fraude, error y omisión de los controles de SI.					
ORIENTACIÓN	La separación de funciones y áreas de responsabilidad tiene como objetivo separar las responsabilidades conflictivas entre diferentes individuos a fin de evitar que ejecuten posibles deberes conflictivos por su cuenta. La organización debería determinar qué deberes y áreas de responsabilidad deberían ser segregadas. A continuación, se muestran ejemplos de actividades que pueden requerir separación: a) inicio, aprobación y ejecución de un cambio; b) solicitud, aprobación y aplicación de los derechos de acceso; c) diseño, implementación y revisión del código; d) desarrollo de software y administración de sistemas de producción; e) utilización y administración de aplicaciones; f) utilización de aplicaciones y administración de bases de datos; g) diseño, auditoría y garantía de los controles de SI. Al diseñar la segregación se debería tener en cuenta la posibilidad de colusión. Las organizaciones pequeñas pueden encontrar difícil lograr la separación de obligaciones, pero el principio se debería aplicar siempre que sea posible y factible. Cuando sea difícil separar, se deberían considerar otros controles, como el seguimiento de las actividades, los registros de auditoría y la supervisión de la dirección. Cuando se utilicen sistemas de control de acceso basados en roles, hay que tener cuidado de que no se concedan a las personas funciones contradictorias. 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 se deberían definir y aprovisionar cuidadosamente para minimizar los problemas de acceso si se elimina o se reasigna un rol.					
OTRA IN-	No hay más información.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

FORMACIÓN	

5.4. RESPONSABILIDADES DE GESTIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Gobierno**	**#Gobierno_y_ecosistema**	**7.2.1**
CONTROL	La administración debería exigirle a todo el personal que aplique la SI de acuerdo con la política de SI establecida, las políticas y los procedimientos específicos de cada tema.					
PROPÓSITO	Garantizar que la dirección comprenda su papel en la SI y emprender acciones encaminadas a garantizar que todo el personal sea consciente y cumpla con sus responsabilidades en materia de SI.					
ORIENTACIÓN	La administración debería demostrar el apoyo a la política de SI, a las políticas específicas de cada tema, a los procedimientos y a los controles de SI. Las responsabilidades de la dirección deberían incluir la garantía de que el personal: a) está debidamente informado sobre sus roles y responsabilidades de SI antes de que se le conceda acceso a la información de la organización y a otros activos asociados; b) ha recibido orientaciones respecto a las expectativas de SI de su rol; c) tiene el mandato de cumplir la política de SI y las políticas específicas de cata tema; d) logra un nivel de sensibilización sobre la SI pertinente para sus roles y responsabilidades (ver 6.3); e) cumpla los términos y condiciones de empleo, contrato o acuerdo, que comprende la política de SI y los métodos de trabajo apropiados; f) siga teniendo las habilidades y calificaciones apropiadas de SI a través de la educación profesional continua; g) cuando sea factible, tenga un canal confidencial para informar sobre violaciones de la política de SI, políticas específicas de cada tema o procedimientos para la SI (“denuncia”). Esto puede permitir la presentación de informes anónimos o tener disposiciones para garantizar que el conocimiento de la identidad del informante sea conocido solo por aquellos que necesiten ocuparse de dichos informes; h) cuente con recursos adecuados y tiempo de planificación de proyectos para implementar los procesos y controles relacionados con la SI.					
OTRA INFORMACIÓN	No hay más información.					

5.5. CONTACTO CON AUTORIDADES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Correctivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Proteger #Responder #Recuperar**	**#Gobierno**	**#Defensa #Resiliencia**	**6.1.3**
CONTROL	La organización debería establecer y mantener contacto con las autoridades pertinentes.					
PROPÓSITO	Garantizar un flujo de información adecuado con respecto a la SI entre la organización y las autoridades legales, reglamentarias y de supervisión pertinentes.					
ORIENTACIÓN	La organización debería especificar cuándo y por quién se debería contactar a las autoridades (por ejemplo, las autoridades encargadas de hacer cumplir la ley, los organismos reguladores, las autoridades supervisoras) y cómo deberían informarse oportunamente los incidentes de SI identificados. Los contactos con las autoridades también se deberían utilizar para facilitar la comprensión de las expectativas actuales y futuras de estas autoridades (por ejemplo, las normas					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	aplicables de SI).
OTRA INFORMACIÓN	Las organizaciones atacadas pueden solicitar a las autoridades que tomen medidas contra la fuente del ataque. El mantenimiento de estos contactos puede ser un requisito para respaldar la gestión de incidentes de SI (ver 5.24 a 5.28) o los procesos de planificación de contingencias y continuidad del negocio (ver 5.29 y 5.30). Los contactos con los organismos reguladores también son útiles para anticipar y prepararse para los próximos cambios en las leyes o reglamentos pertinentes que afectan a la organización. Los contactos con otras autoridades incluyen los servicios públicos, los servicios de emergencia, los proveedores de electricidad y la salud y la seguridad; por ejemplo, los departamentos de bomberos (en conexión con la continuidad de las operaciones), proveedores de telecomunicaciones (en relación con el enrutamiento y la disponibilidad de las líneas) y proveedores de agua (en relación con las instalaciones de refrigeración de equipos).

5.6. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Corrección	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger #Responder #Recuperar**	**#Gobierno**	**#Defensa**	**6.1.4**
CONTROL	La organización debería establecer y mantener contacto con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.					
PROPÓSITO	Garantizar que se produce un flujo adecuado de información con respecto a la SI.					
ORIENTACIÓN	La pertenencia a grupos o foros de interés especial debería considerarse como un medio para: a) mejorar el conocimiento sobre las mejores prácticas y mantenerse al día con la información de seguridad pertinente; b) asegurarse de que la comprensión del entorno de SI es mantiene actualizada; c) recibir alertas tempranas, avisos y parches relacionados con ataques y vulnerabilidades; d) obtener acceso a asesoramiento especializado en SI; e) compartir e intercambiar información sobre nuevas tecnologías, productos, servicios, amenazas o vulnerabilidades; f) proporcionar puntos de enlace adecuados cuando se trate de incidentes de SI (ver 5.24 al 5.28).					
OTRA INFORMACIÓN	No hay más información.					

5.7. INTELIGENCIA SOBRE AMENAZAS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Detectivo #Corrección	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Detectar #Responder**	**#Gestión_de_amenazas_y_vulnerabilidades**	**#Defensa #Resiliencia**	**Nuevo**
CONTROL	La información relativa a las amenazas a la SI se debería recopilar y analizar para producir inteligencia sobre amenazas.					
PROPÓSITOS	Dar a conocer el entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas.					
ORIENTACIÓN	Se debería recopilar y analizar información sobre amenazas existentes o emergentes para: a) facilitar acciones informadas para evitar que las amenazas causen daños; b) reducir el impacto de tales amenazas. La inteligencia frente a amenazas se debería considera en tres capas: a) inteligencia de amenazas estratégicas: intercambio de información de alto nivel sobre el cambiante panorama de amenazas (por ejemplo, tipos de atacantes o tipos de ataques); b) inteligencia de amenazas tácticas: información sobre metodologías, herramientas y					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	tecnologías de atacantes implicadas; c) inteligencia operativa sobre amenazas: detalles sobre ataques específicos, incluidos indicadores técnicos. La inteligencia frente a amenazas debería ser: a) pertinente (es decir, relacionado con la protección de la organización); b) perspicaz (es decir, proporcionar a la organización una comprensión precisa y detallada del panorama de amenazas); c) contextual, para proporcionar conciencia situacional (es decir, agregar contexto a la información basada en el momento de los eventos, donde ocurren, experiencias previas y prevalencia en organizaciones similares); d) procesable (es decir, la organización puede actuar sobre la información de forma rápida y eficaz). Las actividades de inteligencia frente a amenazas deberían incluir: a) establecer objetivos para la producción de inteligencia frente a amenazas; b) identificar, determinar y seleccionar fuentes de información internas y externas que sean necesarias y apropiadas para proporcionar la información necesaria para la producción de inteligencia frente a amenazas; c) recopilar información de fuentes seleccionadas, que pueden ser internas y externas; d) procesar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o corroborando la información); e) analizar la información para entender cómo se relaciona y es significativa para la organización; f) comunicarla y compartirla con los individuos pertinentes en un formato que pueda ser entendido. Se debería analizar y utilizar la inteligencia de amenazas posteriormente: a) mediante la implementación de procesos para incluir información recopilada de fuentes de inteligencia frente a amenazas en los procesos de gestión de riesgos de SI; b) como aporte adicional a los controles técnicos preventivos y detectivos, como firewalls, sistemas de detección de intrusiones o soluciones antimalware; c) como aportación a los procesos y técnicas de prueba de SI. La organización debería compartir la inteligencia sobre amenazas con otras organizaciones de forma mutua a fin de mejorar la inteligencia general sobre amenazas.
OTRA INFORMACIÓN	Las organizaciones pueden utilizar la inteligencia frente a amenazas para prevenir, detectar o responder a las amenazas. Las organizaciones pueden producir inteligencia frente a amenazas, pero normalmente reciben y utilizan la inteligencia frente a amenazas producida por otras fuentes. La inteligencia sobre amenazas es a menudo proporcionada por proveedores o asesores independientes, agencias gubernamentales o grupos de inteligencia sobre amenazas colaborativos. La eficacia de los controles como los descritos en 5.25, 8.7, 8.16 o 8.23, depende de la calidad de la información disponible sobre las amenazas.

5.8. SI EN LA GESTIÓN DE PROYECTOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Proteger**	**#Gobierno**	**#Gobierno_y_ecosistema #Protección**	**6.1.5 14.1.1**
CONTROL	La SI se debería integrar en la gestión de proyectos.					
PROPÓSITO	Garantizar que los riesgos de SI relacionados con los proyectos y los productos finales se aborden de forma eficaz en la gestión de proyectos durante todo el ciclo de vida del proyecto.					
ORIENTACIÓN	La SI se debería integrar en la gestión de proyectos para garantizar que los riesgos de SI se aborden como parte de la gestión del proyecto. Esto se puede aplicar a cualquier tipo de proyecto independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación (por ejemplo, un proyecto para un proceso organizacional principal, TIC, gestión de instalaciones u otros procesos de soporte). La gestión de proyectos en uso debería exigir que: a) los riesgos de SI se evalúen y traten en una fase temprana y periódicamente como parte de los riesgos del proyecto a lo largo del ciclo de vida del proyecto; b) los requisitos de SI (por ejemplo, requisitos de seguridad de las aplicaciones (ver 8.26), requisitos para					

	el cumplimiento de los derechos de propiedad intelectual (ver 5.32), etc.) se aborden en las primeras etapas de los proyectos; c) los riesgos de SI asociados con la ejecución de proyectos, como la seguridad de los aspectos de comunicación interna y externa, se consideren y traten a lo largo del ciclo de vida del proyecto; d) se revise el progreso en el tratamiento de riesgos de SI y se evalúe y prueba la eficacia del tratamiento. La idoneidad de las consideraciones y actividades de SI debería ser seguida en etapas predefinidas por personas u órganos de gobierno adecuados, como el comité directivo del proyecto. Las responsabilidades y autoridades de SI pertinentes para el proyecto se deberían definir y asignar a funciones específicas. Los requisitos de SI para los productos o servicios que el proyecto debería proporcionar se deberían determinar mediante varios métodos, incluidos los requisitos de cumplimiento derivados de la política de SI, y las políticas y las normativas específicas de cada tema. Se pueden obtener requisitos adicionales de SI a partir de actividades como la modelación de amenazas, las revisiones de incidentes, el uso de umbrales de vulnerabilidad o la planificación de contingencias, garantizando así que la arquitectura y el diseño de los sistemas de información estén protegidos contra amenazas conocidas basadas en el entorno operativo. Los requisitos de SI se deberían determinar para todos los tipos de proyectos, no solo para los proyectos de desarrollo de las TIC. Al determinar estos requisitos también se debería tener en cuenta lo siguiente: a) qué información está implicada (determinación de la información), cuáles son las necesidades de SI correspondientes (clasificación; ver 5.12) y el impacto negativo potencial en el negocio que puede resultar de la falta de seguridad adecuada; b) las necesidades de protección requeridas de la información y otros activos asociados involucrados, particularmente en términos de confidencialidad, integridad y disponibilidad; c) el nivel de confianza o garantía necesario para la identidad reclamada de las entidades con el fin de obtener los requisitos de autenticación; d) acceder a los procesos de provisión y autorización, tanto para clientes como para otros posibles usuarios organizacionales, así como para usuarios con privilegios o técnicos, como los miembros relevantes del proyecto, el personal de operaciones potencial o los proveedores externos; e) informar a los usuarios de sus deberes y responsabilidades; f) los requisitos derivados de los procesos organizacionales, como el registro y la supervisión de transacciones, los requisitos de no rechazo; g) requisitos exigidos por otros controles de SI (por ejemplo, interfases para el registro y la supervisión o sistemas de detección de fugas de datos); h) el cumplimiento del entorno legal, legal, reglamentario y contractual en el que opera la organización; i) nivel de confianza o garantía requerido para que terceros cumplan la política de SI de la organización y las políticas específicas de temas, incluidas las cláusulas de seguridad pertinentes en cualquier acuerdo o contrato.
OTRA INFORMACIÓN	El enfoque de desarrollo del proyecto, como el ciclo de vida en cascada o el ciclo de vida ágil, debería apoyar la SI de una manera estructurada que se pueda adaptar a la gravedad evaluada de los riesgos de SI, en función del carácter del proyecto. La consideración temprana de los requisitos de SI para el producto o servicio (por ejemplo, en las etapas de planificación y diseño) puede conducir a soluciones más eficaces y rentables para la calidad y la SI. Las normas ISO 21500 e ISO 21502 proporcionan guía sobre conceptos y procesos de gestión que son importantes para el desempeño de los proyectos. La norma ISO/IEC 27005 proporciona guía sobre el uso de procesos de gestión de riesgos para identificar controles que cumplan con los requisitos de SI.

5.9. INVENTARIO DE ACTIVOS DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Gestión_de_activos**	**#Protección #Gobierno_y_ecosistema**	**8.1.1 8.1.2**
CONTROL	Se debería elaborar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.					
PROPÓSITO	Identificar la información de la organización y otros activos asociados para preservar su SI y asignar la propiedad apropiada.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ORIENTACIÓN	**Inventario** La organización debería identificar su información y otros activos asociados y determinar su importancia en términos de SI. La documentación se debería mantener en inventarios dedicados o existentes, según corresponda. El inventario de información y otros activos asociados debería ser preciso, actualizado, coherente y alineado con otros inventarios. Las opciones para garantizar la exactitud de un inventario de información y otros activos asociados incluyen: a) realizar revisiones periódicas de la información identificada y otros activos asociados con respecto al inventario de activos; b) aplicar automáticamente una actualización de inventario en el proceso de instalación, cambio o eliminación de un activo. La ubicación de un activo se debería incluir en el inventario según corresponda. No es necesario que el inventario sea una lista única de información y otros activos asociados. Tomando en consideración que el inventario se debería mantener por las funciones pertinentes, se puede considerar como un conjunto de inventarios dinámicos, como inventarios de activos de información, hardware, software, máquinas virtuales (VM), instalaciones, personal, competencia, capacidades y registros. Cada activo se debería clasificar de conformidad con la clasificación de la información (ver 5.12) asociada a dicho activo. La granularidad del inventario de información y otros activos asociados debería ser a un nivel apropiado para las necesidades de la organización. A veces no es posible documentar casos específicos 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 asignarse a un individuo o a un grupo y debería identificarse la clasificación (ver 5.12, 5.13). Se debería implementar un proceso para asegurar la asignación oportuna de la propiedad de los activos. La propiedad se debería asignar cuando se crean activos o cuando se transfieren a la organización. La propiedad de activos se debería reasignar según sea necesario cuando los propietarios de activos actuales abandonen o cambien las funciones del trabajo. **Obligaciones del propietario** El propietario del activo debería ser responsable de la correcta gestión de un activo durante todo el ciclo de vida del activo y garantizar que: a) se realiza el inventario de la información y otros activos asociados; b) la información y otros activos asociados se clasifican y protegen adecuadamente; c) la clasificación se revisa periódicamente; d) se enumeran y vinculan componentes que respaldan activos tecnológicos, como bases de datos, almacenamiento, componentes de software y subcomponentes; e) se establecen requisitos para el uso aceptable de la información y otros activos asociados (ver 5.10); f) las restricciones de acceso corresponden a la clasificación y son efectivas y se revisan periódicamente; g) la información y otros activos asociados, cuando se eliminan o eliminan, se gestionan de forma segura y se eliminan del inventario; h) participa en la identificación y gestión de los riesgos asociados a sus activos; i) apoya al personal que tiene las funciones y responsabilidades de gestionar su información.
OTRA INFORMACIÓN	Los inventarios de información y otros activos asociados son a menudo necesarios para garantizar la protección eficaz de la información y pueden ser necesarios para otros fines, como salud y seguridad, seguros o razones financieras. Los inventarios de información y otros activos asociados también apoyan 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 se pueden delegar (por ejemplo, a un custodio que se encarga de los activos diariamente), pero la persona o grupo que los delegó sigue siendo responsable. Puede ser útil designar grupos de información y otros activos asociados que actúen conjuntamente para proporcionar un servicio en particular. En este caso, el propietario de este servicio es responsable de la prestación del servicio, incluido el funcionamiento de sus activos. Información adicional sobre la gestión de activos de TI en la norma ISO/IEC 19770-1. Información adicional sobre la gestión de activos en la norma ISO 55001.

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

5.10. USO ACEPTABLE DE LA INFORMACIÓN Y LOS ACTIVOS ASOCIADOS

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Gobierno_y_ecosistema #Protección	8.1.3 8.2.3
CONTROL	Se deberían identificar, documentar y aplicar normas 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 estén protegidos, utilizados y gestionados de forma adecuada.					
ORIENTACIÓN	El personal y los usuarios externos que utilicen o tengan acceso a la información de la organización y a otros activos asociados deberían ser conscientes de los requisitos de SI para proteger y manejar la información de la organización y otros activos asociados. Deberían ser responsables del uso de cualquier servicio de procesamiento de 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 la información y otros activos asociados. La política específica sobre el uso aceptable debería proporcionar una guía clara sobre cómo se espera que los individuos utilicen la información y otros activos asociados. La política específica del tema debería indicar: a) comportamientos esperados e inaceptables desde la perspectiva de SI; b) uso permitido y prohibido de la información y otros activos asociados; c) seguimiento de las actividades realizadas por la organización. Se deberían elaborar procedimientos de uso aceptables para el ciclo de vida completo de la información de acuerdo con su clasificación (ver 5.12) y los riesgos determinados. Se deberían tomar en consideración los siguientes factores: a) restricciones de acceso que apoyen los requisitos de protección para cada nivel de clasificación; b) mantenimiento de un registro de los usuarios autorizados de la información y otros activos asociados; c) protección de copias temporales o permanentes de la información a un nivel compatible con la protección de la información original; d) almacenamiento de los activos asociados a la información de conformidad con las especificaciones de los fabricantes (Ver 7.8); e) marcado claro de todas las copias de los medios de almacenamiento (electrónicos o físicos) a la atención del destinatario autorizado (ver 7.10); f) autorización de la eliminación de la información y otros activos asociados y método(s) de eliminación admitido(s) (Ver 8.10).					
OTRA INFORMACIÓN	Puede ocurrir que los activos afectados no pertenezcan directamente a la organización, como los servicios de nube pública. El uso de activos de terceros y de cualquier activo de la organización asociado con dichos activos externos (por ejemplo, información, software) se debería identificar como aplicable y controlarse, por ejemplo, mediante acuerdos con proveedores de servicios en la nube. También se debería tener cuidado cuando se utiliza un entorno de trabajo colaborativo.					

5.11. DEVOLUCIÓN DE ACTIVOS

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos	#Protección	8.14
CONTROL	El personal y otras partes interesadas, según corresponda, deberían devolver todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

PROPÓSITO	Proteger los activos de la organización como parte del proceso de cambio o terminación de empleo, contrato o acuerdo.
ORIENTACIÓN	El proceso de cambio o terminación debería formalizarse para incluir la devolución de todos los activos físicos y electrónicos emitidos anteriormente que sean propiedad de la organización o que se hayan confiado a ella. En los casos en que el personal y otras partes interesadas adquieran el equipo de la organización o utilicen su propio equipo personal, se deberían seguir los procedimientos necesarios para garantizar que toda la información relevante se rastree y transfiera a la organización y se elimine de forma segura del equipo (ver 7.14). En los casos en que el personal y otras partes interesadas tengan conocimientos importantes para las operaciones en curso, esa información se debería documentar y transferir a la organización. Durante el período de notificación y posteriormente, la organización debería evitar la copia no autorizada de la información relevante (por ejemplo, propiedad intelectual) por parte del personal previo aviso de terminación. La organización debería identificar y documentar claramente toda la información y otros activos asociados que se devolverán, que pueden incluir: a) dispositivos finales del usuario; b) dispositivos de almacenamiento portátiles; c) equipo especializado; d) hardware de autenticación (por ejemplo, claves mecánicas, tokens físicos y tarjetas inteligentes) para sistemas de información, sitios y archivos físicos; e) copias físicas de la información
OTRA INFORMACIÓN	Puede ser difícil devolver información contenida en activos que no son propiedad de la organización. En tales casos, es necesario restringir el uso de la información al utilizar otros controles de SI como la gestión de derechos de acceso (ver 5.18) o el uso de criptografía (ver 8.24).

5.12. CLASIFICACIÓN DE LA INFORMACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Protección_de_la_información**	**#Protección #Defensa**	**8.2.1**
CONTROL	La información se debería clasificar según las necesidades de SI de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.					
PROPÓSITO	Asegurar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.					
ORIENTACIÓN	La organización debería establecer una política específica sobre clasificación de la información y comunicarla a todas las partes interesadas pertinentes, teniendo en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación. Las clasificaciones y los controles de protección asociados para la información deberían tener en cuenta las necesidades organizacionales para compartir o restringir la información, para proteger su integridad y para asegurar su disponibilidad, así como los requisitos legales relativos a la confidencialidad, integridad o disponibilidad de la información. Los activos distintos de la información también se pueden clasificar de acuerdo con la clasificación de la información, que se almacena, procesa o gestiona o protege con el activo. Los propietarios de la información deberían ser responsables de su clasificación. El esquema de clasificación debería incluir convenciones para la clasificación y criterios para la revisión de la clasificación a lo largo del tiempo. Los resultados de la clasificación deberían actualizarse de acuerdo con los cambios en el valor, la sensibilidad y la criticidad de la información a lo largo de su ciclo de vida. El esquema debería estar alineado con la política específica sobre control de acceso (ver 5.1) y debería ser capaz de abordar las necesidades organizacionales específicas. La clasificación puede determinarse por el nivel de impacto que el compromiso de la información tendría para la organización. A cada nivel definido en el esquema se le debería dar un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación. El sistema debería ser coherente en toda la organización e incluirse en sus procedimientos					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	para que todos clasifiquen la información y otros activos asociados aplicables de la misma manera. De esta manera, todos tienen una comprensión común de los requisitos de protección y aplican una protección adecuada. El esquema de clasificación utilizado puede ser diferente de los esquemas utilizados por otras organizaciones, incluso si los nombres de los niveles son similares. Además, la información se mueve entre las organizaciones pueden variar en clasificación dependiendo de su contexto en cada organización, incluso si sus esquemas de clasificación son idénticos. Por lo tanto, los acuerdos con otras organizaciones que 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 los distintos regímenes puede determinarse buscando la equivalencia en los métodos de manipulación y protección asociados.
OTRA INFORMACIÓN	La clasificación proporciona a las personas que se ocupan de la información una indicación concisa de cómo manejarla y protegerla. Esto se facilita mediante la creación de grupos de información con necesidades de protección similares y la especificación de procedimientos de SI que se aplican a toda la información de cada grupo. Este enfoque reduce la necesidad de una evaluación de riesgos caso por caso y un diseño personalizado de controles. La información puede dejar de ser sensible o crítica después de un cierto período de tiempo. Por ejemplo, cuando la información se ha hecho pública ya no tiene requisitos de confidencialidad, pero puede requerir protección para sus propiedades de integridad y disponibilidad. Estos aspectos deberían tenerse en cuenta ya que la excesiva clasificación puede conducir a la aplicación de controles innecesarios que producen gastos adicionales o, por el contrario, la subclasificación puede conducir a controles insuficientes para proteger la información de compromisos. Como ejemplo, un esquema de clasificación de confidencialidad de la información puede basarse en cuatro niveles como sigue: a) la divulgación no causa ningún daño; b) la divulgación causa daños menores a la reputación o un menor impacto operativo; c) la divulgación tiene un impacto significativo a corto plazo en las operaciones o los objetivos organizacionales; d) la divulgación tiene un impacto grave en los objetivos organizacionales a largo plazo o pone en riesgo la supervivencia de la organización

5.13. ETIQUETADO DE LA INFORMACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Protección_de_la_información**	**#Defensa #Protección**	**8.2.2**
CONTROL	Debería elaborarse y aplicarse un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el plan de clasificación de la información adoptado.					
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 para el etiquetado de la información deberían abarcar la información y otros activos asociados en todos los formatos. El etiquetado debería reflejar el sistema de clasificación establecido en 5.12. Las etiquetas deberían ser fácilmente reconocibles. Los procedimientos deberían proporcionar guía sobre dónde y cómo se adjuntan las etiquetas en consideración de cómo se accede a la información o cómo se manejan los activos dependiendo de los tipos de medios de almacenamiento. Los procedimientos pueden definir: a) casos en los que se omite el etiquetado (por ejemplo, etiquetado de información no confidencial para reducir las cargas de trabajo); b) cómo etiquetar la información enviada o almacenada por medios electrónicos o físicos o en cualquier otro formato; c) cómo manipular los casos en los que no es posible el etiquetado (por ejemplo, debido a restricciones técnicas). Entre los ejemplos de técnicas de etiquetado se incluyen: a) etiquetas físicas; b) encabezados y pies de página; c) metadatos;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	d) marcas de agua; e) sellos de goma. La información digital debería utilizar metadatos para identificar, gestionar y controlar la información, especialmente en lo que respecta a la confidencialidad. Los metadatos también deberían permitir una búsqueda eficaz y correcta de la información. Los metadatos deberían facilitar la interacción de los sistemas y la toma de decisiones basadas en las etiquetas de clasificación asociadas. Los procedimientos deberían describir cómo adjuntar metadatos a la información, qué etiquetas utilizar y cómo deberían manejarse los datos, de acuerdo con el modelo de información y la arquitectura de las TIC de la organización. Los sistemas deberían agregar metadatos adicionales relevantes cuando procesan la información en función de sus propiedades de SI. El personal y otras partes interesadas deberían tener conocimiento de los procedimientos de etiquetado. Se debería proporcionar a todo el personal la formación necesaria para garantizar que la información está correctamente etiquetada y manejada en consecuencia. La salida de los sistemas que contienen información clasificada como sensible o crítica debería llevar una etiqueta de clasificación adecuada.
OTRA INFORMACIÓN	El etiquetado de la información clasificada es un requisito clave para el intercambio de información. Otros metadatos útiles que se pueden adjuntar a la información son qué proceso organizativo creó la información y en qué momento. El etiquetado de la información y otros activos asociados a veces puede tener efectos negativos. Los activos clasificados pueden ser más fáciles de identificar por parte de actores malintencionados para un posible uso indebido. Algunos sistemas no etiquetan archivos individuales o registros de bases de datos con su clasificación, sino que protegen toda la información al nivel más alto de clasificación de cualquier información que contiene o que se permite que contenga. En estos sistemas es habitual determinar y etiquetar la información cuando se exporta.

5.14. TRANSFERENCIA DE INFORMACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_activos #Protección_de_la_información**	**#Protección**	**13.2.1 13.2.2 13.2.3**
CONTROL	Se deberían establecer normas, procedimientos o acuerdos de transferencia de información para todos los tipos de facilidades de transferencia dentro de la organización y entre la organización y otras partes.					
PROPÓSITOS	Mantener la SI transferida dentro de una organización y con cualquier parte externa interesada.					
ORIENTACIÓN	**General** La organización debería establecer y comunicar a todas las partes interesadas una política específica de transferencia de información. Las normas, procedimientos y acuerdos para proteger la información en tránsito deberían reflejar la clasificación de la información en cuestión. Cuando la información se transfiere entre la organización y terceros, se deberían establecer y mantener acuerdos de transferencia (incluida la autenticación del destinatario) para proteger la información en todas las formas en tránsito (ver 5.10). La transferencia de información puede realizarse mediante transferencia electrónica, transferencia de medios de almacenamiento físico y transferencia verbal. Para todos los tipos de transferencia de información, las normas, procedimientos y acuerdos deberían incluir: a) controles diseñados para proteger la información transferida de intercepciones, accesos no autorizados, copias, modificaciones, rutas incorrectas, destrucción y denegación de servicio, incluidos los niveles de control de acceso acordes con la clasificación de la información implicada y cualquier control especial que se requiera para proteger la información confidencial, como el uso de técnicas cifradas (ver 8.24); b) controles para garantizar la trazabilidad y el no rechazo, incluido el mantenimiento de una cadena de custodia de la información durante el tránsito; c) identificación de los contactos apropiados relacionados con la transferencia, incluidos					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	los propietarios de la información, los propietarios de riesgos, los oficiales de seguridad y los custodios de la información, según corresponda; d) responsabilidades y obligaciones en caso de incidentes de SI, como la pérdida de medios de almacenamiento físicos o datos; e) el uso de un sistema de etiquetado acordado para información sensible o crítica, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información esté debidamente protegida (ver 5.13); f) fiabilidad y disponibilidad del servicio de transferencia; g) la política o directrices específicas sobre el uso aceptable de los servicios de transferencia de la información (ver 5.10); h) directrices de retención y eliminación para todos los registros organizacionales, incluidos los mensajes; NOTA: Puede existir legislación y regulaciones locales en relación con la retención y eliminación de registros comerciales. i) la consideración de cualquier otro requisito legal, estatutario, reglamentario y contractual relevante (ver 5.31, 5.32, 5.33 y 5.34) relacionado con la transferencia de información (por ejemplo, requisitos para firmas electrónicas). **Transmisión electrónica** Cuando se utilicen medios de comunicación electrónica para la transferencia de información, las normas, procedimientos y acuerdos también deberían considerar lo siguiente: a) detección y protección contra malware que se puede transmitir mediante el uso de comunicaciones electrónicas (ver 8.7); b) protección de la información electrónica confidencial comunicada en forma de anexo; c) prevención contra el envío de documentos y mensajes en comunicaciones a direcciones o números incorrectos; d) aprobación antes de utilizar servicios públicos externos como mensajería instantánea, redes sociales, uso compartido de archivos o almacenamiento en la nube; e) autenticación a niveles más sólidos al transferir información a través de redes de acceso público; f) restricción asociada a las instalaciones de comunicación electrónica (por ejemplo, evitar la automatización reenvío de correo electrónico a direcciones de correo externas); g) consejos al personal y a otras partes interesadas de no enviar mensajes SMS (servicio de mensajes cortos) o mensajes instantáneos con información crítica ya que pueden leerse en lugares públicos (y por lo tanto por personas no autorizadas) o almacenarse en dispositivos que no estén protegidos adecuadamente; h) asesoría al personal y a otras partes interesadas sobre los problemas del uso de máquinas o servicios de fax, a saber: 1) acceso no autorizado a almacenes de mensajes integrados para recuperar mensajes; 2) programación deliberada o accidental de máquinas para enviar mensajes a números específicos. **Transmisión en medios de almacenamiento físico** Al transferir medios de almacenamiento físicos (incluido el papel), las reglas, procedimientos y acuerdos también deberían incluir: a) responsabilidades de control y notificación de la transmisión, envío y recepción; b) correcto direccionamiento y transporte del mensaje; c) embalaje que proteja el contenido de cualquier daño físico que se pueda producir durante el transporte y de acuerdo con las especificaciones del fabricante, por ejemplo, protección contra cualquier factor medioambiental que pueda reducir la eficacia de la restauración de los medios de almacenamiento, como la exposición al calor, la humedad o los campos electromagnéticos; utilizar normas técnicas mínimas para el embalaje y la transmisión (por ejemplo, el uso de sobres opacos); d) lista de correos fiables autorizados acordada por la dirección; e) normas de identificación de mensajería; f) controles a prueba de manipulaciones (por ejemplo, bolsas, contenedores) en función del nivel de clasificación de la información en el medio de almacenamiento que se va a transportar; g) procedimientos para verificar la identificación de los correos; h) lista aprobada de terceros que proporcionan servicios de transporte o mensajería en función de la clasificación de la información; i) registros para identificar el contenido de los medios de almacenamiento, la protección aplicada, así como registrar la lista de destinatarios autorizados, los tiempos de

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	transferencia a los custodios de tránsito y la recepción en el destino. **Transmisión verbal** Para proteger la transmisión verbal de información, se debería recordar al personal y a otras partes interesadas que deben: a) evitar conversaciones verbales confidenciales en lugares públicos o a través de canales de comunicación inseguros ya que pueden ser escuchadas por personas no autorizadas; b) evitar dejar mensajes que contengan información confidencial en los contestadores automáticos o mensajes de voz ya que pueden ser reproducidos por personas no autorizadas, almacenados en sistemas comunitarios o almacenados incorrectamente como resultado de un marcado erróneo; c) seleccionar al nivel apropiado para escuchar la conversación; d) asegurar que se implementan los controles adecuados en la sala (por ejemplo, aislamiento acústico, puerta cerrada); e) comenzar cualquier conversación sensible con un descargo de responsabilidad para que los presentes conozcan el nivel de clasificación y cualquier requisito de manejo de lo que están a punto de oír.
OTRA INFORMACIÓN	No hay más información.

5.15. CONTROL DE ACCESO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_la_identidad_y_del_acceso**	**#Protección**	**9.1.1 9.1.2**
CONTROL	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deberían establecerse e implementarse en función de los requisitos de SI y del negocio.					
PROPÓSITO	Garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.					
ORIENTACIÓN	Los propietarios de la información y otros activos asociados deberían determinar la SI y los requisitos organizacionales relacionados con el control de acceso. Debería definirse una política específica sobre el control del acceso que tenga en cuenta estos requisitos y debería comunicarse a todas las partes interesadas pertinentes. Estos requisitos y la política específica del tema deberían considerar lo siguiente: a) identificación de que entidades requieren qué tipo de acceso a la información y otros activos asociados; b) seguridad de las aplicaciones (ver 8.26); c) acceso físico, que debería estar soportado por los controles de entrada físicos apropiados (ver 7.2, 7.3 y 7.4); d) difusión y autorización de la información (por ejemplo, el principio de necesidad de conocer) y niveles de SI y clasificación de la información (ver 5.10, 5.12 y 5.13); e) restricciones al acceso privilegiado (ver 8.2); f) segregación de deberes (ver 5.3); g) legislación, reglamentos y obligaciones contractuales pertinentes relativas a la limitación del acceso a datos o servicios (ver 5.31, 5.32, 5.33, 5.34 y 8.3); h) segregación de las funciones de control de acceso (por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso); i) autorización formal de solicitudes de acceso (ver 5.16 y 5.18); j) gestión de los derechos de acceso (ver 5.18); k) registro (ver 8.15). Las reglas de control de acceso deberían implementarse definiendo y mapeando los derechos y restricciones de acceso apropiados a las entidades pertinentes (ver 5.16). Una entidad puede representar a un usuario humano, así como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio). Para simplificar la gestión del control de acceso, se pueden asignar roles específicos a los grupos de entidades. Al definir e implementar las reglas de control de acceso, se debería tener en cuenta: a) la coherencia entre los derechos de acceso y la clasificación de la información; b) la coherencia entre los derechos de acceso y las necesidades y requisitos de seguridad					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	del perímetro físico; c) todos los tipos de conexiones disponibles en los entornos distribuidos para que las entidades solo tengan acceso a la información y otros activos asociados, incluidas las redes y los servicios de red, que estén autorizados a utilizar; d) cómo se pueden reflejar los elementos o factores relevantes para el control dinámico de acceso.
OTRA INFORMACIÓN	A menudo se utilizan principios generales en el contexto del control de acceso. Dos de los principios más utilizados son: a) necesidad de saber: a una entidad solo se le concede acceso a la información que requiere para realizar sus tareas (diferentes tareas o funciones significan una información diferente de necesidad de saber y, por lo tanto, diferentes perfiles de acceso); b) necesidad de uso: a una entidad solo se le asigna acceso a la infraestructura de tecnología de la información cuando existe una necesidad clara. Al especificar las reglas de control de acceso se debería tener en cuenta: a) establecer reglas basadas en la premisa del menor privilegio, "Todo está generalmente prohibido a menos que esté expresamente permitido", en lugar de la regla más débil, "Todo está generalmente permitido a menos que esté expresamente prohibido"; b) los cambios en las etiquetas de información (ver 5,13) que se inician automáticamente mediante las instalaciones de procesamiento de información y los iniciados a discreción del usuario; c) los cambios en los permisos de usuario iniciados automáticamente por el sistema de información y los iniciados por un administrador; d) cuando definir y revisar regularmente la aprobación. Las reglas de control de acceso deberían estar respaldadas por procedimientos documentados (ver 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5 y 8.18) y definición de responsabilidades (ver 5.2 y 5.17). Existen varias formas de implementar el control de acceso, como MAC (control de acceso obligatorio), DAC (control de acceso discrecional), RBAC (control de acceso basado en roles) y ABAC (control de acceso basado en atributos). Las reglas de control de acceso también pueden contener elementos dinámicos (por ejemplo, una función que evalúa accesos pasados o valores de entorno específicos). Las reglas de control de acceso se pueden implementar en diferente granularidad, desde la cobertura de redes o sistemas completos hasta campos de datos específicos y también pueden considerar propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso. Estos principios y cómo se define el control de acceso granular pueden tener un impacto significativo en los costes. Las reglas más sólidas y una mayor granularidad normalmente conducen a un mayor costo. Los requisitos organizacionales 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

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_la_identidad_y_del_acceso**	**#Protección**	**9.2.1**
CONTROL	Se debería gestionar todo el ciclo de vida de las identidades.					
PROPÓSITO	Permitir la identificación única de individuos y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.					
ORIENTACIÓN	Los procesos utilizados en el contexto de la gestión de identidades deberían garantizar que: a) para las identidades asignadas a personas, una identidad específica solo está vinculada a una sola persona para que pueda responsabilizar a la persona de las acciones realizadas con esta identidad específica; b) las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por motivos organizacionales u operativos y están sujetas a aprobación y documentación específicas; c) las identidades asignadas a entidades no humanas están sujetas a una aprobación					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	debidamente segregada y a una supervisión independiente continua; d) las identidades se desactivan o eliminan de forma oportuna si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se utilizan o si la persona vinculada a una identidad ha abandonado la organización o ha cambiado el rol); e) en un dominio específico, se asigna una única identidad a una sola entidad, [es decir, se evita la asignación de varias 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 usuario 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 re-verificación de documentos de confianza relacionados con una persona. Al utilizar identidades proporcionadas o emitidas por terceros (por ejemplo, credenciales de redes sociales), la organización debería asegurarse de que las identidades de terceros proporcionan el nivel de confianza necesario y de que se conocen y tratan suficientemente los riesgos asociados. Esto puede incluir controles relacionados con terceros (ver 5.19), así como controles relacionados con la información de autenticación asociada (ver 5.17).
OTRA INFORMACIÓN	Proporcionar o revocar el acceso a la información y otros activos asociados suele ser un procedimiento de varios pasos: a) confirmar los requisitos organizacionales para establecer una identidad; b) verificar la identidad de una entidad antes de asignarles una identidad lógica; c) establecer una identidad; d) configurar y activar la identidad. Esto también incluye la configuración y configuración inicial de los servicios de autenticación relacionados; e) proporcionar o revocar derechos de acceso específicos a la identidad, sobre la base de las decisiones de autorización o derecho apropiadas (Ver 5.18).

5.17. INFORMACIÓN DE AUTENTICACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_la_identidad_y_del_acceso**	**#Protección**	**9.2.4 9.3.1 9.4.3**
CONTROL	La asignación y gestión de la información de autenticación debería controlarse mediante un proceso de gestión, que incluya el asesoramiento del personal sobre el tratamiento adecuado de la información de autenticación.					
PROPÓSITO	Garantizar la correcta autenticación de entidades y evitar errores en los procesos de autenticación.					
ORIENTACIÓN	**<u>Asignación de información de autenticación</u>** El proceso de asignación y gestión debería garantizar que: a) las contraseñas personales o los números de identificación personal (PIN) generados automáticamente durante los procesos de inscripción es información de autenticación secreta temporal que no se puede adivinar y es única para cada persona y los usuarios deberían cambiarlos después del primer uso; b) se establecen procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación nueva, de sustitución o temporal; c) la información de autenticación, incluida la información de autenticación temporal, se transmite a los usuarios de forma segura (por ejemplo, a través de un canal autenticado y protegido) y se evita el uso de mensajes de correo electrónico no protegidos (texto no cifrado) con este fin; d) los usuarios acusan recibo de la información de autenticación; e) la información de autenticación predeterminada predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de sistemas o software; f) se mantienen registros de eventos significativos relativos a la asignación y gestión de la información de autenticación y se otorga su confidencialidad y se aprueba el método de mantenimiento de registros (por ejemplo, mediante el uso de una herramienta de almacén de contraseñas aprobada). **<u>Responsabilidades del usuario</u>**					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Cualquier persona que tenga acceso o utilice la información de autenticación debería ser aconsejada para asegurarse de que: a) la información de autenticación secreta, como las contraseñas, se mantiene confidencial. La información de autenticación secreta personal no debería compartirse con nadie. La información de autenticación secreta utilizada en el contexto de identidades vinculadas a varios 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 la notificación o cualquier otra indicación de un compromiso; c) cuando se utilizan contraseñas como información de autenticación, se seleccionan contraseñas seguras según las recomendaciones de prácticas recomendadas, por ejemplo: 1) las contraseñas no se basen en nada que otra persona pueda adivinar u obtener fácilmente al utilizar información relacionada con la persona (por ejemplo, nombres, números de teléfono y fechas de nacimiento); 2) las contraseñas no se basen en palabras de diccionario o sus combinaciones; 3) se utilicen frases de contraseña fáciles de recordar e intente incluir caracteres alfanuméricos y especiales; 4) las contraseñas tienen una longitud mínima; d) las mismas contraseñas no se utilizan en distintos servicios y sistemas; e) la obligación de seguir estas normas también se incluye en términos y condiciones de empleo (ver 6.2). **Sistema de gestión de contraseñas** Cuando se utilizan contraseñas como información de autenticación, el sistema de gestión de contraseñas debe: a) permitirles a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para solucionar los errores de entrada; b) aplicar contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas (ver c) “Responsabilidades del usuario”); c) forzar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión; d) aplicar los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad o al terminar o cambiar de empleo cuando un usuario tiene contraseñas conocidas para identidades que permanecen activas (por ejemplo, identidades compartidas); e) evitar la reutilización de contraseñas anteriores; f) evitar el uso de contraseñas de uso común y nombres de usuario comprometidos, combinaciones de contraseñas de sistemas pirateados; g) no mostrar contraseñas en la pantalla al introducirlas; h) almacene y transmita contraseñas en forma protegida. El cifrado de contraseñas y el hashing deberían realizarse de acuerdo con las técnicas cifradas aprobadas para contraseñas (ver 8.24).
OTRA INFORMACIÓN	Las contraseñas o frases de acceso son un tipo de información de autenticación que se utiliza habitualmente y son un medio común de verificar la identidad de un usuario. Otros tipos de información de autenticación son las claves cifradas, los datos almacenados en tokens de hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación y datos biométricos, como escaneos de iris o huellas dactilares. Información adicional en la norma ISO/IEC 24760. Requerir cambios frecuentes de contraseñas puede ser problemático porque los usuarios se pueden molestar por los cambios frecuentes olvidar contraseñas nuevas, anotarlas en lugares inseguros o elegir contraseñas no seguras. La provisión de inicio de sesión único (SSO) u otras herramientas de administración de autenticación (por ejemplo, almacenes de contraseñas) reduce la cantidad de información de autenticación que los usuarios deberían proteger y, por lo tanto, puede aumentar la eficacia de este control. Sin embargo, estas herramientas también pueden aumentar el impacto de la revelación de información de autenticación. Algunas aplicaciones requieren que una autoridad independiente asigne contraseñas de usuario. En tales casos, a), c) y d) del sistema de gestión de contraseñas no se aplican.

5.18. DERECHOS DE ACCESO

ATRIBUTOS	Tipo de	Propiedades de la	Conceptos de	Capacidades	Dominios de	CONTROLES

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Control	SI	Ciberseguridad	operativas	Seguridad	ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_la_identidad_y_del_acceso	#Protección	9.2.2 9.2.5 9.2.6
CONTROL	Los derechos de acceso a la información y a otros activos asociados se deberían proveer, revisar, modificar y eliminar de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.					
PROPÓSITO	Garantizar que el acceso a la información y otros activos asociados se define y autoriza de acuerdo con los requisitos organizacionales.					
ORIENTACIÓN	**Provisión y revocación de derechos de acceso** El proceso para asignar o revocar derechos de acceso físicos y lógicos otorgados a la identidad autenticada de una entidad debería incluir: a) obtención de la autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados (ver 5.9). También puede ser apropiada la aprobación por separado de los derechos de acceso por parte de la administración; b) consideración de los requisitos organizacionales y la política y las reglas específicas de cada tema de la organización sobre el control de acceso; c) consideración de la separación de deberes, que incluye la separación de las funciones de aprobación e implementación de los derechos de acceso y la separación de roles conflictivos; d) garantía de que se eliminan los derechos de acceso 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 abandonado la organización se eliminan de forma oportuna; e) consideración de la concesión de derechos de acceso temporal durante un período de tiempo limitado y su revocación en la fecha de vencimiento, en particular para el personal temporal o el acceso temporal requerido por el personal; f) verificación de que el nivel de acceso concedido se ajuste a las políticas específicas del tema sobre control de acceso (ver 5.15) y sea coherente con otros requisitos de SI, como la separación de funciones (ver 5.3); g) garantía de que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de que los procedimientos de autorización se hayan completado correctamente; h) mantención de un registro central de los derechos de acceso otorgados a un identificador de usuario (ID, lógico o físico) para acceder a la información y otros activos asociados; i) modificación de los derechos de acceso de los usuarios que han cambiado de roles o trabajos; j) eliminación o ajuste de los derechos de acceso físicos y lógicos, que se pueden realizar mediante la eliminación, revocación o sustitución de claves, información de autenticación, tarjetas de identificación o suscripciones; k) mantención de un registro de los cambios en los derechos de acceso lógicos y físicos de los usuarios. **Revisión de los derechos de acceso** Las revisiones periódicas de los derechos de acceso físicos y lógicos deberían tener en cuenta lo siguiente: a) los derechos de acceso de los usuarios después de cualquier cambio en la misma organización (por ejemplo, cambio de empleo, ascenso, descenso) o terminación del empleo (ver 6.1 a 6.5); b) las autorizaciones para derechos de acceso privilegiados. Consideración antes del cambio o la terminación del empleo Los derechos de acceso de un usuario a la información y otros activos asociados deberían revisarse y ajustarse o eliminarse antes de cualquier cambio o cese del empleo basándose en la evaluación de factores de riesgo como: a) si la terminación o el cambio es iniciado por el usuario o por la dirección y el motivo de la terminación; b) las responsabilidades actuales del usuario; c) el valor de los activos actualmente accesibles.					
OTRA IN-	Se debería tener en cuenta el establecimiento de funciones de acceso de usuarios en función					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

FORMACIÓN	de los requisitos organizacionales que resumen una norma de derechos de acceso en perfiles de acceso de usuarios típicos. Las solicitudes de acceso y las revisiones de los derechos de acceso se gestionan más fácilmente en el nivel de dichas funciones que en el nivel de derechos concretos. Se debería considerar la inclusión de cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta acceder sin autorización (ver 5.20, 6.2, 6.4 y 6.6). En los casos de terminación iniciada por la administración, el personal descalificado o los usuarios externos pueden dañar deliberadamente la información o sabotear las instalaciones de procesamiento de la información. En los casos de personas que se refirman o son despedidas, pueden verse tentadas a recoger información para uso futuro. La clonación es una forma eficaz de que las organizaciones asignen acceso a los usuarios. Sin embargo, debería hacerse con cuidado basado en funciones distintas identificadas por la organización en lugar de clonar una identidad con todos los derechos de acceso asociados. La clonación tiene un riesgo inherente de resultar en derechos de acceso excesivos a la información y otros activos asociados.

5.19. SI EN LAS RELACIONES CON LOS PROVEEDORES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Seguridad_de_las_relaciones_con_proveedores**	**#Gobierno_y_ecosistema #Protección**	**15.1.1**
CONTROL	Deberían definirse e implementarse procesos y procedimientos para gestionar los riesgos de SI asociados con el uso de los productos o servicios del proveedor.					
PROPÓSITO	Mantener un nivel acordado de SI 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 por parte de la organización de los recursos de los proveedores de servicios en la nube. Estos procesos y procedimientos deberían incluir aquellos que debería implementar la organización, así como aquellos que la organización requiere que el proveedor implemente para el inicio del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor, tales como: a) identificar y documentar los tipos de proveedores (por ejemplo, Servicios de TIC, logística, servicios públicos, servicios financieros, componentes de infraestructura de TIC) que pueden afectar a la confidencialidad, integridad y disponibilidad de la información de la organización; b) establecer cómo evaluar y seleccionar proveedores según la sensibilidad de la información, los productos y los servicios (por ejemplo, con análisis de mercado, referencias de clientes, revisión de documentos, evaluaciones in situ, certificaciones); c) evaluar y seleccionar los productos o servicios del proveedor que tengan controles adecuados de SI y revisarlos; en particular, la exactitud e integridad de los controles implementados por el proveedor que garanticen la integridad de la información del proveedor y el procesamiento de la información y, por lo tanto, la SI 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 y servicios de la infraestructura de TIC proporcionados por los proveedores que puedan afectar a la confidencialidad, integridad y disponibilidad de la información de la organización; f) evaluar y gestionar los riesgos de SI asociados con: 1) el uso por parte de los proveedores de la información de la organización y otros activos asociados, incluidos los riesgos originados por el personal potencialmente malintencionado de los proveedores; 2) el mal funcionamiento o las vulnerabilidades de los productos (incluidos los componentes y subcomponentes de software utilizados en estos productos) o los servicios					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	prestados por los proveedores; g) supervisar el cumplimiento de los requisitos de SI establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por parte de terceros y la validación del producto; h) mitigar la no conformidad de un proveedor, tanto si se ha detectado a través de la supervisión como por otros medios; i) manejar incidentes y contingencias asociados con productos y servicios del proveedor, incluyendo responsabilidades tanto de la organización como de los proveedores; j) desarrollar resiliencia y, si es necesario, medidas de recuperación y contingencia para asegurar la disponibilidad de la información y el procesamiento de la información del proveedor y, por ende, la disponibilidad de la información de la organización; k) sensibilizar y formar al personal de la organización que interactúa con el personal de los proveedores en lo que respecta a las normas de compromiso adecuadas, las políticas, los procesos y los procedimientos específicos y el comportamiento en función del tipo de proveedor y del nivel de acceso del proveedor a los sistemas y la información de la organización; l) gestionar la necesaria transferencia de información, de otros activos asociados y de cualquier otro elemento que deba modificarse y garantizar el mantenimiento de la SI durante todo el periodo de transferencia; m) definir los requisitos para garantizar una terminación segura de la relación con el proveedor, que incluye: 1) retiro de los derechos de acceso; 2) tratamiento de la información; 3) titularidad de la propiedad intelectual desarrollada durante el compromiso; 4) portabilidad de la información en caso de cambio de proveedor o de recurso interno (insourcing); 5) gestión de documentos; 6) devolución de activos; 7) eliminación segura de la información y otros activos asociados; 8) requisitos de confidencialidad continuos; n) definir el nivel de seguridad del personal y seguridad física que se espera del personal y las instalaciones del proveedor. Los 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 debido a los avances tecnológicos) deberían considerarse para evitar cualquier retraso en la organización de productos o servicios de sustitución (por ejemplo, identificando un proveedor alternativo por adelantado o al utilizar siempre proveedores alternativos).
OTRA INFORMACIÓN	En los casos en que no es posible que una organización exija requisitos a un proveedor, la organización debería: a) considerar la guía dada en este control al tomar decisiones sobre la elección de un proveedor y su producto o servicio; b) implementar controles de compensación según sea necesario basándose en una evaluación de riesgos. Los proveedores con una gestión inadecuada de la SI pueden poner en peligro la información. Se deberían determinar y aplicar controles para gestionar el acceso del proveedor a la información y otros activos asociados. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de no divulgación o técnicas de cifrado. Otro ejemplo son los riesgos de protección de datos personales cuando el acuerdo con el proveedor implica la transferencia de información o el acceso a ella a través de las fronteras. La organización debería ser consciente de que la responsabilidad legal o contractual de proteger la información sigue siendo responsabilidad de la organización. Los riesgos también pueden ser causados por controles inadecuados de los componentes de la infraestructura de TIC o de los servicios prestados por los proveedores. Los componentes o servicios vulnerables o que funcionan mal pueden provocar infracciones de la SI en la organización o en otra entidad (por ejemplo, pueden causar infecciones de malware, ataques u otros daños a entidades distintas de la organización). Mas información en la norma ISO/IEC 27036-2.

5.20. ABORDAR LA SI EN LOS ACUERDOS CON LOS PROVEEDORES

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_las_relaciones_con_proveedores	#Gobierno_y_ecosistema #Protección	15.1.2
CONTROL	Los requisitos de SI pertinentes debieran establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.					
PROPÓSITO	Mantener un nivel acordado de SI en las relaciones con los proveedores.					
ORIENTACIÓN	Se deberían establecer y documentar acuerdos con proveedores para garantizar que existe un entendimiento claro entre la organización y el proveedor en relación con las obligaciones de ambas partes de cumplir los requisitos de SI pertinentes. Se pueden considerar los siguientes términos para su inclusión en los acuerdos con el fin de satisfacer los requisitos de SI identificados: a) descripción de la información que se debería proporcionar o acceder a ella y métodos de suministro o acceso a la información; b) clasificación de la información según el esquema de clasificación de la organización (ver 5.10, 5.12 y 5.13); c) correspondencia entre el esquema de clasificación propio de la organización y el esquema de clasificación del proveedor; d) requisitos legales, legales, reglamentarios y contractuales, incluidos la protección de datos, el tratamiento de la IIP, los derechos de propiedad intelectual y los derechos de autor y una descripción de cómo se garantizará su cumplimiento; e) obligación de cada parte contractual de implementar un conjunto acordado de controles, incluyendo control de acceso, revisión de desempeño, monitoreo, informe y auditoría y las obligaciones del proveedor de cumplir con los requisitos de SI organizacionales; f) normas de uso aceptable de la información y otros activos asociados, incluido el uso inaceptable si es necesario; g) procedimientos o condiciones para la autorización y eliminación 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 para utilizar la información organizacional y otros activos asociados); h) requisitos de SI en relación con la infraestructura de TIC del proveedor; en particular, requisitos mínimos de SI para cada tipo de información y tipo de acceso que sirvan de base para los acuerdos de proveedores individuales basados en las necesidades empresariales y los criterios de riesgo de la organización; i) indemnizaciones y reparación por incumplimiento de los requisitos del contratista; j) requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la corrección de incidentes); k) requisitos de formación y concienciación para procedimientos específicos y requisitos de SI (por ejemplo, para la respuesta a incidentes, procedimientos de autorización); l) disposiciones pertinentes para la subcontratación, incluidos los controles que deberían aplicarse, tales como el acuerdo sobre el uso de los subproveedores (por ejemplo, exigir que se cumplan las mismas obligaciones del proveedor, exigir que se disponga de una lista de subproveedores y notificación antes de cualquier cambio); m) contactos pertinentes, incluida una persona de contacto para problemas de SI; n) cualquier requisito de selección, cuando sea legalmente permisible, para el personal del proveedor, incluidas las responsabilidades para llevar a cabo los procedimientos de detección y notificación si no se ha completado la selección o si los resultados dan lugar a dudas o preocupaciones; o) mecanismos de prueba y garantía de las declaraciones de terceros sobre los requisitos pertinentes de SI relacionados con los procesos del proveedor y un informe independiente sobre la eficacia de los controles; p) derecho a auditar los procesos y controles del proveedor relacionados con el acuerdo; q) obligación del proveedor de presentar periódicamente un informe sobre la eficacia de los controles y un acuerdo sobre la corrección oportuna de las cuestiones pertinentes planteadas en el informe; r) resolución de defectos y procesos de resolución de conflictos; s) copias de seguridad alineadas con las necesidades de la organización (en términos de frecuencia, tipo y ubicación de almacenamiento); t) disponibilidad de una instalación alternativa (es decir, un sitio de recuperación ante					

	desastres) que no esté sujeta a las mismas amenazas que la instalación principal y consideraciones para los controles de retorno (controles alternativos) en caso de que fallen los controles principales; u) proceso de gestión de cambios que garantice la notificación anticipada a la organización y la posibilidad de que la organización no acepte cambios; v) controles de seguridad física acordes con la clasificación de la información; w) controles de transferencia de información para proteger la información durante la transferencia física o la transmisión lógica; x) cláusulas de terminación al concluir el acuerdo, incluida la gestión de registros, la devolución de activos, la eliminación segura de la información y otros activos asociados, así como cualquier obligación de confidencialidad en curso; y) suministro de un método para destruir de forma segura la información de la organización almacenada por el proveedor en cuanto ya no sea necesaria; z) garantía, al final del contrato, del traspaso del apoyo a otro proveedor o a la organización misma. La organización debería establecer y mantener un registro de acuerdos con partes externas (por ejemplo, contratos, memorando de entendimiento, acuerdos de intercambio de información) para hacer un seguimiento de dónde va su información. La organización también debería revisar, validar y actualizar regularmente sus acuerdos con partes externas para asegurarse de que siguen siendo necesarios y aptos para su propósito con las cláusulas de SI pertinentes.
OTRA INFORMACIÓN	Los acuerdos pueden variar considerablemente para las distintas organizaciones y entre los distintos tipos de proveedores. Por lo tanto, se debería tener cuidado de incluir todos los requisitos pertinentes para abordar los riesgos de SI. Información más detallada sobre acuerdos con proveedores en la norma ISO/IEC 27036. Información sobre los acuerdos de servicios en la nube en la norma ISO/IEC 19086.

5.21. GESTIÓN DE LA SI EN LA CADENA DE SUMINISTRO TIC

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Seguridad_de_las_relaciones_con_proveedores**	**#Gobierno_y_ecosistema #Protección**	**15.1.3**
CONTROL	Deberían definirse y aplicarse procesos y procedimientos para gestionar los riesgos de SI asociados a la cadena de suministro de productos y servicios de TIC.					
PROPÓSITO	Mantener un nivel acordado de SI en las relaciones con los proveedores.					
ORIENTACIÓN	Se deberían considerar los siguientes temas para abordar la SI dentro de la seguridad de la cadena de suministro de TIC, además de los requisitos generales de SI para las relaciones con los proveedores: a) definir los requisitos de SI que se aplicarán a la adquisición de productos o servicios de TIC; b) exigir que los proveedores de servicios de TIC propaguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro si subcontratan partes del servicio de TIC proporcionado a la organización; c) exigir que los proveedores de productos de TIC propaguen las prácticas de seguridad adecuadas a lo largo de la cadena de suministro si estos productos incluyen componentes comprados o adquiridos a otros proveedores u otras entidades (por ejemplo, desarrolladores de software subcontratados y proveedores de componentes de hardware); d) solicitar a los proveedores de productos TIC que proporcionen información que describa los componentes de software utilizados en los productos; e) solicitar a los proveedores de productos TIC que proporcionen información que describa las funciones de seguridad implementadas de su producto y la configuración necesaria para su funcionamiento seguro; f) implementar un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de TIC entregados cumplan con los requisitos de seguridad establecidos. Ejemplos de dichos métodos de revisión de proveedores pueden incluir pruebas de penetración y pruebas o validación de declaraciones de terceros para las operaciones de SI del proveedor;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	g) implementar un proceso para identificar y documentar los componentes de productos o servicios que son críticos para mantener la funcionalidad y, por lo tanto, requieren mayor atención, escrutinio y seguimiento adicional cuando se crean fuera de la organización, especialmente si el proveedor subcontrata aspectos de los componentes de productos o servicios a otros proveedores; h) obtener la garantía de que los componentes críticos y su origen pueden rastrearse a lo largo de la cadena de suministro; i) obtener la garantía de que los productos TIC suministrados funcionan como se esperaba sin ninguna característica inesperada o no deseada; j) implementar procesos para garantizar que los componentes de los proveedores sean auténticos y no se alteren de sus especificaciones. Entre las medidas de ejemplo se incluyen etiquetas antimanipulación, verificaciones cifradas de hash o firmas digitales. El control para detectar un rendimiento fuera de las especificaciones puede ser un indicador de manipulación o falsificación. La prevención y la detección de manipulación deberían implementarse durante varias etapas del ciclo de vida del desarrollo del sistema, incluidos el diseño, el desarrollo, la integración, las operaciones y el mantenimiento; k) obtener la garantía de que los productos TIC alcanzan los niveles de seguridad requeridos, por ejemplo, mediante una certificación formal o un esquema de evaluación como el Acuerdo Común de Reconocimiento de Criterios; l) definir reglas para compartir información sobre la cadena de suministro y cualquier posible problema y compromiso entre la organización y los proveedores; m) implementar procesos específicos para gestionar el ciclo de vida y la disponibilidad de los componentes de TIC y los riesgos de seguridad asociados. Esto incluye la gestión de los riesgos de que los componentes ya no estén disponibles debido a que los proveedores ya no están en el negocio o a que los proveedores ya no proporcionan estos componentes debido a los avances tecnológicos. Debería considerarse la identificación de un proveedor alternativo y el proceso de transferencia de software y competencia al proveedor alternativo.
OTRA INFORMACIÓN	Las prácticas específicas de gestión de riesgos de la cadena de suministro de TIC se basan en prácticas generales de SI, calidad, gestión de proyectos e ingeniería de sistemas, pero no las sustituyen. Se aconseja a las organizaciones que trabajen con los proveedores para comprender la cadena de suministro de TIC y cualquier asunto que tenga un efecto importante en los productos y servicios que se proporcionan. La organización puede influir en las prácticas de SI de la cadena de suministro de TIC al dejar en claro en los acuerdos con sus proveedores los asuntos que deberían abordar otros proveedores de la cadena de suministro de TIC. Las TIC deberían adquirirse de fuentes de confianza. La fiabilidad del software y del 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 confiables basados en la reputación del proveedor. La cadena de suministro de TIC, tal como se aborda aquí, incluye servicios en la nube. Ejemplos de cadenas de suministro de TIC son: a) aprovisionamiento de servicios en la nube, donde el proveedor de servicios en la nube depende de los desarrolladores de software, los proveedores de servicios de telecomunicaciones y los proveedores de hardware; b) IoT, donde el servicio implica a los fabricantes de dispositivos, a los proveedores de servicios en la nube (por ejemplo, los operadores de plataforma IoT), los desarrolladores de aplicaciones móviles y web, el proveedor de bibliotecas de software; c) servicios de alojamiento, en los que el proveedor depende de escritorios de servicio externos, incluidos el primero, el segundo y el tercer nivel de soporte. Para obtener más detalles, incluida la guía de evaluación de riesgos, ver la norma ISO/IEC 27036-3. Las etiquetas de identificación de software (SWID) también pueden ayudar a lograr una mejor SI en la cadena de suministro, proporcionando información sobre la procedencia del software. Más información en la norma ISO/IEC 19770-2.

5.22. SEGUIMIENTO, REVISIÓN Y GESTIÓN DE CAMBIOS DE LOS SERVICIOS DE LOS PROVEEDORES

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013

	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Seguridad_de_las_relaciones_con_proveedores**	**#Gobierno_y_ecosistema #Seguridad_de_la_información**	**15.2.1 15.2.2**
CONTROL	La organización debería supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de SI del proveedor y en la prestación de servicios.					
PROPÓSITO	Mantener un nivel acordado de SI y prestación de servicios de acuerdo con los acuerdos con los proveedores.					
ORIENTACIÓN	La supervisión, revisión y gestión de cambios de los servicios de proveedores debería garantizar el cumplimiento de los términos y condiciones de SI de los acuerdos, la gestión adecuada de los incidentes y problemas de SI y los cambios en los servicios de proveedores o en el estado empresarial no afectan a la prestación de servicios. Esto debería implicar un proceso para gestionar la relación entre la organización y el proveedor para: a) supervisar los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos; b) supervisar los cambios realizados por los proveedores, entre los que se incluyen: 1) mejoras en los servicios actuales ofrecidos; 2) desarrollo de cualquier aplicación y sistema nuevos; 3) modificaciones o actualizaciones de las políticas y procedimientos del proveedor; 4) controles nuevos o modificados para resolver incidentes de SI y mejorar la SI; c) supervisar los cambios en los servicios del proveedor, incluidos: 1) cambios y mejoras en las redes; 2) utilización de nuevas tecnologías; 3) adopción de nuevos productos o versiones o versiones más recientes; 4) nuevas herramientas y entornos de desarrollo; 5) cambios en la ubicación física de las instalaciones de servicio; 6) cambio de subproveedores; 7) subcontratación con otro proveedor; d) revisar los informes de servicio producidos por el proveedor y organizar reuniones periódicas de progreso según lo requerido por los acuerdos; e) llevar a cabo auditorías de proveedores y subproveedores, junto con la revisión de los informes de auditores independientes, si están disponibles y el seguimiento de las cuestiones identificadas; f) proporcionar información sobre incidentes de SI y revisar esta información según lo requieran los acuerdos y las directrices y procedimientos de apoyo; g) revisar los registros de auditoría de proveedores y los registros de eventos de SI, problemas operativos, fallas, seguimiento de fallas e interrupciones relacionados con el servicio prestado; h) responder y gestionar cualquier incidente o evento de SI identificado; i) identificar las vulnerabilidades de SI y gestionarlas; j) revisar los aspectos de SI de las relaciones del proveedor con sus propios proveedores; k) asegurar que el proveedor mantenga una capacidad de servicio suficiente junto con planes viables diseñados para garantizar que se mantienen los niveles de continuidad del servicio acordados tras fallas de servicio o desastres importantes (ver 5.29, 5.30, 5.35, 5.36, 8.14); l) asegurar que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos; m) evaluar regularmente que los proveedores mantienen niveles adecuados de SI. La responsabilidad de gestionar las relaciones con los proveedores debería asignarse a un individuo o equipo designado. Deberían ponerse a disposición suficientes conocimientos técnicos y recursos para supervisar que se cumplen los requisitos del acuerdo, en particular los requisitos de SI. Se deberían tomar las medidas adecuadas cuando se observen deficiencias en la prestación de servicios.					
OTRA INFORMACIÓN	Más información en la norma ISO/IEC 27036-3.					

5.23. SI PARA EL USO DE SERVICIOS EN LA NUBE

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_relaciones_con_proveedores**	**#Gobierno_y_ecosistema #Protección**	**Nuevo**
CONTROL	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deberían establecerse de acuerdo con los requisitos de SI de la organización.					
PROPÓSITO	Especificar y gestionar la SI para el uso de servicios en la nube.					
ORIENTACIÓN	La organización debería establecer y comunicar una política específica sobre el uso de los servicios en la nube a todas las partes interesadas. La organización debería definir y comunicar cómo pretende gestionar los riesgos de SI asociados con el uso de servicios en la nube. Puede ser una extensión o parte del enfoque existente para la forma en que una organización administra los servicios prestados por partes externas (ver 5.21 y 5.22). El uso de los servicios en la nube puede implicar una responsabilidad compartida en materia de SI y un esfuerzo de colaboración entre el proveedor de servicios en la nube y la organización que actúa como cliente de dichos servicios. Es esencial que las responsabilidades tanto del proveedor de servicios en la nube como de la organización, que actúa como cliente de los servicios en la nube, se definan y apliquen adecuadamente. La organización debería definir: a) todos los requisitos de SI pertinentes asociados con el uso de los servicios en la nube; b) criterios de selección de servicios en la nube y alcance del uso del servicio en la nube; c) funciones y responsabilidades relacionadas con el uso y la gestión de servicios en la nube; d) qué controles de SI son gestionados por el proveedor de servicios en la nube y que son gestionados por la organización como cliente del servicio en la nube; e) cómo obtener y utilizar las capacidades de SI proporcionadas por el proveedor de servicios en la nube; f) cómo obtener la garantía de los controles de SI implementados por los proveedores de servicios en la nube; g) cómo gestionar controles, interfaces y cambios en los servicios cuando una organización utiliza varios servicios en la nube, especialmente de distintos proveedores de servicios en la nube; h) procedimientos para gestionar los incidentes de SI que se producen en relación con el uso de servicios en la nube; i) su enfoque para supervisar, revisar y evaluar el uso continuo de los servicios en la nube para gestionar los riesgos de SI; j) cómo cambiar o detener el uso de los servicios en la nube, incluidas las estrategias de salida de los servicios en la nube. Los acuerdos de servicios en la nube suelen estar predefinidos y no están abiertos a la negociación. Para todos los servicios en la nube, la organización debería revisar los acuerdos de servicios en la nube con los proveedores de servicios en la nube. Un acuerdo de servicio en la nube debería abordar los requisitos de confidencialidad, integridad, disponibilidad y gestión de la información de la organización, con los objetivos de nivel de servicio en la nube y los objetivos cualitativos del servicio en la nube adecuados. La organización también debería realizar evaluaciones de riesgos pertinentes para identificar los riesgos asociados con el uso del servicio en la nube. Cualquier riesgo residual relacionado con el uso del servicio en la nube debería ser claramente identificado y aceptado por la dirección apropiada de la organización. Un acuerdo entre el proveedor de servicios en la nube y la organización, que actúa como cliente de servicios en la nube, debería incluir las siguientes disposiciones para la protección de los datos de la organización y la disponibilidad de los servicios: a) proporcionar soluciones basadas en normas aceptadas aceptados en el sector para arquitectura e infraestructura; b) gestionar los controles de acceso del servicio en la nube para satisfacer los requisitos de la organización; c) implementar soluciones de protección y supervisión de malware; d) procesar y almacenar la información confidencial de la organización en lugares aprobados (por ejemplo, un país o región en particular) o dentro de una jurisdicción determinada o sujeta a ella; e) proporcionar asistencia especializada en caso de que se produzca un incidente de SI en el entorno de servicios en la nube;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	f) garantizar que se cumplen los requisitos de SI de la organización en caso de que los servicios en la nube se subcontraten a un proveedor externo (o prohibir la subcontratación de servicios en la nube); g) apoyar a la organización en la recopilación de pruebas digitales, tomando en consideración las leyes y normativas para pruebas digitales en diferentes jurisdicciones; h) proporcionar soporte y disponibilidad adecuados de los servicios para un plazo de tiempo adecuado cuando la organización desea salir del servicio en la nube; i) proporcionar la copia de seguridad necesaria de los datos y la información de configuración y gestionar de forma segura las copias de seguridad según corresponda, en función de las capacidades del proveedor de servicios en la nube que utiliza la organización, al actuar como cliente del servicio en la nube; j) proporcionar y devolver información como archivos de configuración, código fuente y datos que son propiedad de la organización, actuando como cliente del servicio en la nube, cuando se solicite durante la prestación del servicio o al finalizar el servicio. La organización, que actúa como cliente del servicio en la nube, debería considerar si el acuerdo debería exigir a los proveedores de servicios en la nube que proporcionen una notificación previa antes de que cualquier cambio importante afecte la forma en que se entrega el servicio a la organización, incluidos: a) cambios en la infraestructura técnica (por ejemplo, reubicación, reconfiguración o cambios en hardware o software) que afectan o modifican la oferta de servicios en la nube; b) procesar o almacenar información en una nueva jurisdicción geográfica o jurídica; c) uso de proveedores de servicios en la nube de pares u otros subcontratistas (incluido el cambio de proveedores existentes o el uso de nuevos proveedores). La organización que utiliza servicios en la nube debería mantener un estrecho contacto con sus proveedores de servicios en la nube. Estos contactos permiten el intercambio mutuo de información sobre la SI para el uso de los servicios en la nube, que incluye un mecanismo para que tanto el proveedor de servicios en la nube como la organización, actúen como cliente del servicio en la nube, supervisen cada característica del servicio e informen de fallas de los compromisos contenidos en los acuerdos.
OTRA INFORMACIÓN	Este control considera la seguridad de la nube desde la perspectiva del cliente del servicio de nube. Información adicional sobre los servicios en la nube en las normas ISO/IEC 17788, ISO/IEC 17789 e ISO/IEC 22123-1. Información relacionada con la portabilidad de la nube en apoyo de las estrategias de salida en la norma ISO/IEC 19941. Información relacionada con la SI y los servicios de nube pública en la norma ISO/IEC 27017. Detalles relacionados con la protección IIP en nubes públicas que actúan como procesador de IIP en la norma ISO/IEC 27018. Las relaciones con los proveedores de servicios en la nube en la ISO/IEC 27036-4 y los acuerdos de servicios en la nube y su contenido en la norma ISO/IEC 19086, con seguridad y privacidad específicamente cubiertas por la ISO/IEC 19086-4.

5.24. PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SI

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Corrección	**#Confidencialidad #Integridad #Disponibilidad**	**#Responder #Recuperar**	**#Gobierno #Gestión_de_eventos_de_SI**	**#Defensa**	**16.1.1**
CONTROL	La organización debería planificar y prepararse para gestionar los incidentes de SI definiendo, estableciendo y comunicando los procesos, funciones y responsabilidades de gestión de incidentes de SI.					
PROPÓSITO	Garantizar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de SI, incluida la comunicación sobre los eventos de SI.					
ORIENTACIÓN	**<u>Funciones y responsabilidades</u>** La organización debería establecer procesos apropiados de gestión de incidentes de SI. Las funciones y responsabilidades para llevar a cabo los procedimientos de gestión de incidentes deberían determinarse y comunicarse eficazmente a las partes interesadas internas y externas pertinentes. Se debería considerar: a) establecer un método común para informar sobre eventos de SI, que incluye el punto de					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	contacto (Ver 6.8); b) establecer un proceso de gestión de incidentes de SI para proporcionar a la organización la capacidad de gestionarlos, que incluya la administración, documentación, detección, clasificación, priorización, análisis, comunicación y coordinación de las partes interesadas; c) establecer un proceso de respuesta a incidentes para proporcionar a la organización la capacidad de evaluar, responder y aprender de los incidentes de SI; d) permitir que el personal competente se encargue de los problemas relacionados con los incidentes de SI dentro de la organización. Dicho personal debería recibir documentación sobre procedimientos y capacitación periódica; e) establecer un proceso para identificar la formación, la certificación y el desarrollo profesional continuo necesarios para el personal de respuesta a incidentes. **Procedimientos de gestión de incidentes** Los objetivos de la gestión de incidentes de SI deberían acordarse con la administración y se debería asegurar que los responsables de la gestión de incidentes de SI comprendan las prioridades de la organización para gestionarlos, que incluya el marco temporal de resolución basado en las consecuencias y la gravedad potenciales. Se deberían implementar procedimientos de gestión de incidentes para cumplir con estos objetivos y prioridades. La administración debería asegurarse de que se cree un plan de gestión de incidentes de SI tomando en consideración los diferentes escenarios y procedimientos que se desarrollen e implementen para las siguientes actividades: a) evaluación de los eventos de SI según criterios para lo que constituye un incidente de SI; b) vigilancia (ver 8.15 y 8.16), detección (ver 8.16), clasificación (ver 5.25), análisis e informes (ver 6.8) de los eventos e incidentes de SI (por medios humanos o automáticos); c) gestión de los incidentes de SI hasta su conclusión, incluida la respuesta y el escalamiento (ver 5.26), según el tipo y la categoría del incidente, posible activación de la gestión de crisis y activación de planes de continuidad, recuperación controlada de un incidente y comunicación con partes interesadas internas y externas; d) coordinación con partes interesadas internas y externas, tales como autoridades, grupos y foros de interés externos, proveedores y clientes (ver 5.5 y 5.6); e) registro de actividades de gestión de incidentes; f) gestión de pruebas (ver 5.28); g) análisis de la causa raíz o procedimientos post mortem; h) identificación de las lecciones aprendidas y cualquier mejora en los procedimientos de gestión de incidentes o en los controles de SI en general que sean necesarios. **Procedimientos de presentación de informes** Los procedimientos de presentación de informes deberían incluir: a) acciones a tomar en caso de un evento de SI (por ejemplo, anotar todos los detalles pertinentes inmediatamente, como la aparición de errores de funcionamiento y mensajes en pantalla, informar inmediatamente al punto de contacto y solo tomar acciones coordinadas); b) uso de formularios de incidentes para ayudar al personal a realizar todas las acciones necesarias al informar de incidentes de SI; c) procesos de retroalimentación adecuados para garantizar que las personas que informan sobre eventos de SI sean notificadas, en la medida de lo posible, de los resultados una vez que se ha abordado y cerrado el problema; d) creación de informes de incidentes. Cualquier requisito externo sobre la notificación de incidentes a las partes interesadas pertinentes dentro del plazo definido (por ejemplo, los requisitos de notificación de infracciones a los reguladores) debería ser considerado al implementar los procedimientos de gestión de incidentes.
OTRA INFORMACIÓN	Los incidentes de SI pueden trascender las fronteras organizativas y nacionales. Para responder a tales incidentes, es conveniente coordinar la respuesta y compartir información sobre estos incidentes con organizaciones externas, según corresponda. Una guía detallada sobre la gestión de incidentes de SI en norma ISO/IEC 27035.

5.25. EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SI

ATRIBUTOS	Tipo de	Propiedades de la	Conceptos de	Capacidades	Dominios de	CONTROLES

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Control	SI	Ciberseguridad	operativas	Seguridad	ISO/IEC 27002:2013
	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Ges-tión_de_even-tos_de_SI	#Defensa	16.1.4
CONTROL	La organización debería evaluar los eventos de SI y decidir si se deberían clasificar como incidentes de SI.					
PROPÓSITO	Garantizar la categorización y priorización efectivas de los eventos de SI.					
ORIENTA-CIÓN	Debería acordarse un esquema de categorización y priorización de los incidentes de SI para la identificación de las consecuencias y la prioridad de un incidente. El esquema debería incluir los criterios para clasificar los eventos como incidentes de SI. El punto de contacto debería evaluar cada evento de SI al utilizar el esquema acordado. El personal responsable de coordinar y responder a los incidentes de SI debería realizar la evaluación y tomar una decisión sobre los eventos de SI. Los resultados de la evaluación y la decisión deberían registrarse en detalle a efectos de futuras referencias y verificación.					
OTRA IN-FORMACIÓN	Más guía sobre la gestión de incidentes de SI en la norma ISO/IEC 27035.					

5.26. RESPUESTA A INCIDENTES DE SI

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Corrección	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gobierno #Ges-tión_de_even-tos_de_SI	#Defensa	16.1.5
CONTROL	Los incidentes de SI deberían responderse en conformidad con los procedimientos documentados.					
PROPÓSITO	Garantizar una respuesta eficaz a los incidentes de SI.					
ORIENTA-CIÓN	La organización debería establecer y comunicar los procedimientos de respuesta a incidentes de SI a todas las partes interesadas pertinentes. Los incidentes de SI deberían ser respondidos por un equipo designado con la competencia requerida (ver 5.24). La respuesta debería incluir lo siguiente: a) sistemas afectados, si las consecuencias del incidente pueden extenderse; b) recopilación de evidencias (ver 5.28) lo antes posible, después de la ocurrencia; c) escalamiento, según sea necesario, que incluya actividades de gestión de crisis y posiblemente invocando planes de continuidad de negocio (ver 5.29 y 5.30); d) garantía de que todas las actividades de respuesta implicadas se registran correctamente para su posterior análisis; e) comunicación de la existencia del incidente de SI o de cualquier detalle pertinente a todas las partes interesadas internas y externas pertinentes según el principio de necesidad de saber; f) coordinación con las partes internas y externas como autoridades, grupos de interés y foros externos, proveedores y clientes para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones; g) cierre formal y registro una vez que el incidente ha sido abordado con éxito; h) análisis forenses de SI, según sea necesario (ver 5.28); i) análisis post-incidente para identificar la causa raíz. Asegurarse de que se documente y comunique de acuerdo con los procedimientos definidos (ver 5.27); j) identificación y gestión de las vulnerabilidades y debilidades de SI, lo que incluye las relacionadas con los controles que han causado, contribuido o no han podido prevenir el incidente.					
OTRA IN-FOR-MACIÓN	Más guía sobre la gestión de incidentes en la norma ISO/IEC 27035.					

5.27. APRENDIZAJE DE LOS INCIDENTES DE SI

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Proteger**	**#Ges-tión_de_even-tos_de_SI**	**#Defensa**	**16.1.6**
CONTROL	Los conocimientos obtenidos de los incidentes de SI deberían utilizarse para reforzar y mejorar los controles de SI.					
PROPÓSITO	Reducir la probabilidad de ocurrencia o las consecuencias de futuros incidentes.					
ORIENTA-CIÓN	La organización debería establecer procedimientos para cuantificar y supervisar los tipos, volúmenes y costos de los incidentes de SI. La información obtenida de la evaluación de incidentes de SI debería utilizarse para: a) mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos de incidentes (ver 5.24); b) identificar incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de SI de la organización y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o consecuencias de futuros incidentes similares. Mecanismos que permitan recopilar, cuantificar y supervisar información sobre tipos, volúmenes y costes de incidentes; c) mejorar el conocimiento y la formación de los usuarios (ver 6.3) proporcionando ejemplos de lo que puede suceder, cómo responder a dichos incidentes y cómo evitarlos en el futuro.					
OTRA IN-FORMACIÓN	Más guía sobre la gestión de incidentes en la norma ISO/IEC 27035.					

5.28. RECOPILACIÓN DE EVIDENCIAS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades ope-rativas**	**Dominios de Se-guridad**	**CONTROLES ISO/IEC 27002:2013**
	#Corrección	**#Confidencialidad #Integridad #Disponibilidad**	**#Detectar #Responder**	**#Ges-tión_de_even-tos_de_SI**	**#Defensa**	**16.1.7**
CONTROL	La organización debería establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencias relacionadas con eventos de SI.					
PROPÓSITO	Garantizar una gestión coherente y eficaz de las evidencias relacionadas con los incidentes de SI para los fines de las acciones disciplinarias y legales.					
ORIENTA-CIÓN	Se deberían desarrollar y seguir procedimientos internos cuando se trate de evidencias relacionadas con eventos de SI para los propósitos de acciones disciplinarias y legales. Se deberían considerar los requisitos de las diferentes jurisdicciones para maximizar las posibilidades de admisión en las jurisdicciones pertinentes. En general, estos procedimientos para la gestión de las evidencias deberían proporcionar instrucciones para la identificación, recolección, adquisición y conservación de las evidencias de conformidad con los diferentes tipos de medios de almacenamiento, dispositivos y estado de estos (es decir, encendidos o apagados). Por lo general, las evidencias se deberían recopilar de manera que sean admisibles en los tribunales nacionales correspondientes o en otro foro disciplinario. Debería ser posible demostrar que: a) los registros están completos y no se han manipulado de ninguna manera; b) las copias de las evidencias electrónicas son probablemente idénticas a las originales; c) cualquier sistema de información del que se hayan recopilado evidencia funcionaba correctamente en el momento en que se registraron dichas evidencias. Cuando se disponga de ella, debería buscarse la certificación u otros medios pertinentes de calificación del personal y de los instrumentos, a fin de fortalecer el valor de las evidencias conservadas. La evidencia digital puede trascender los límites organizativos o jurisdiccionales. En tales casos, debería garantizarse que la organización tenga derecho a recopilar la información requerida como prueba digital.					
OTRA IN-FORMACIÓN	Cuando se detecta por primera vez un evento de SI, no siempre es evidente si el evento dará lugar o no a una acción judicial. Por lo tanto, existe el peligro de que las evidencias necesarias se destruyan de forma intencionada o accidental antes de que se comprenda la gravedad del incidente. Se recomienda recurrir al asesoramiento jurídico o a las fuerzas de seguridad en una fase temprana de cualquier acción legal prevista y asesorarse sobre las pruebas necesarias. Definiciones y directrices para la identificación, recopilación, adquisición y conservación de					

	evidencias digitales en la norma ISO/IEC 27037. Guías sobre el descubrimiento electrónico, que implica el procesamiento de información almacenada electrónicamente como evidencia en la norma ISO/IEC 27050.

5.29. SI DURANTE UNA INTERRUPCIÓN

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo #Corrección	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Continuidad	#Protección #Resiliencia	17.1.1 17.1.2 17.1.3
CONTROL	La organización debería planificar cómo mantener la SI en un nivel adecuado durante la interrupción.					
PROPÓSITO	Proteger la información y otros activos asociados durante una interrupción.					
ORIENTACIÓN	La organización debería determinar sus requisitos para adaptar los controles de SI durante una interrupción. Los requisitos de SI deberían incluirse en los procesos de gestión de la continuidad del negocio. Se debería desarrollar, implementar, probar, revisar y evaluar planes para mantener o restaurar la SI de los procesos empresariales críticos tras una interrupción o una falla. La SI debería restaurarse en el nivel requerido y en los plazos requeridos. La organización debería implementar y mantener: a) controles de SI, sistemas y herramientas de apoyo dentro de los planes de continuidad de las empresas y de las TIC; b) procesos para mantener los controles de SI existentes durante una interrupción; c) compensación de los controles de SI que no se pueden mantener durante una interrupción.					
OTRA INFORMACIÓN	En el contexto de la continuidad del negocio y la planificación de la continuidad de las TIC, puede ser necesario adaptar los requisitos de SI en función del tipo de interrupción, en comparación con las condiciones operativas normales. Como parte del análisis del impacto en el negocio y de la evaluación de riesgos realizada dentro de la gestión de la continuidad del negocio, se deberían considerar y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad. Información sobre los sistemas de gestión de la continuidad del negocio en las normas ISO 22301 e ISO 22313. Orientación obre el análisis de impacto empresarial (BIA) en la ISO/TS 22317.					

5.30. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Corrección	#Disponibilidad	#Responder	#Continuidad	#Resiliencia	Nuevo
CONTROL	La preparación para las TIC debería planificarse, implementarse, mantenerse y probarse sobre la base de los objetivos de la continuidad del negocio y los requisitos de continuidad de las TIC.					
PROPÓSITO	Garantizar la disponibilidad de la información de la organización y de otros activos asociados durante una interrupción.					
ORIENTACIÓN	La preparación de las TIC para la continuidad del negocio es un componente importante en la gestión de la continuidad del negocio y la gestión de la SI para garantizar que los objetivos de la organización puedan seguir cumpliéndose durante la interrupción. Los requisitos de continuidad de las TIC son el resultado del análisis de impacto de negocio (BIA, por sus iniciales en inglés). El proceso BIA debería utilizar tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo resultantes de la interrupción de las actividades comerciales que ofrecen productos y servicios. La magnitud y la duración del impacto resultante deberían utilizarse para identificar las actividades prioritarias a las que se debería asignar un objetivo de tiempo de recuperación (RTO). El BIA debería entonces determinar qué recursos se necesitan para apoyar las actividades prioritarias. También debería especificarse un RTO para estos recursos. Un subconjunto de estos recursos debería incluir los servicios de TIC. El BIA que implica servicios de TIC puede ampliarse para definir los requisitos de rendimiento					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	y capacidad de los sistemas de TIC y el punto objetivo de recuperación (RPO) de la información necesaria para apoyar las actividades durante una interrupción. Sobre la base de los resultados del BIA y de la evaluación de riesgos que implican los servicios de TIC, la organización debería identificar y seleccionar estrategias de continuidad de las TIC que consideren opciones para antes, durante y después de una interrupción. Las estrategias de continuidad del negocio pueden incluir una o más soluciones. Sobre la base de las estrategias, se deberían elaborar, aplicar y probar planes para satisfacer el nivel de disponibilidad requerido de los servicios de TIC y en los plazos requeridos luego de una interrupción o la falla de los procesos críticos. La organización debería asegurarse de que: a) se ha establecido una estructura organizativa adecuada para preparar, mitigar y responder a una interrupción apoyada por el personal con la responsabilidad, autoridad y competencia necesarias; b) los planes de continuidad de las TIC, incluidos los procedimientos de respuesta y recuperación en los que se detalla cómo planea la organización gestionar una interrupción del servicio de las TIC, son: 1) periódicamente evaluados mediante ejercicios y pruebas; 2) aprobados por la dirección; c) los planes de continuidad de las TIC incluyen la siguiente información de continuidad de las TIC: 1) especificaciones de rendimiento y capacidad para cumplir los requisitos y objetivos de continuidad del negocio especificados en el BIA; 2) RTO de cada servicio de TIC priorizado y los procedimientos para restaurar esos componentes; 3) RPO de los recursos priorizados de TIC definidos como información y los procedimientos para restaurar la información.
OTRA INFORMACIÓN	La gestión de la continuidad de las TIC es una parte clave de los requisitos de continuidad del negocio relativos a la disponibilidad para poder: a) responder y recuperarse de la interrupción de los servicios de TIC independientemente de la causa; b) asegurar que la continuidad de las actividades prioritarias sea apoyada por los servicios de TIC requeridos; c) responder antes de que se produzca una interrupción de los servicios de TIC y tras la detección de al menos un incidente que pueda provocar una interrupción de los servicios de TIC. Más orientaciones sobre la preparación de las TIC para la continuidad del negocio en la norma ISO/IEC 27031. Más orientaciones sobre los sistemas de gestión de la continuidad del negocio en las normas ISO 22301 e ISO 22313. Más orientaciones sobre el BIA en la norma ISO/TS 22317.

5.31. REQUISITOS LEGALES, REGLAMENTARIOS Y CONTRACTUALES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Legal_y_cumplimiento**	**#Gobierno_y_ecosistema #Protección**	**18.1.1 18.1.5**
CONTROL	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la SI y el enfoque de la organización para cumplir con estos requisitos deberían ser identificados, documentados y actualizados.					
PROPÓSITO	Garantizar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales relacionados con la SI.					
ORIENTACIÓN	**General** Los requisitos externos, incluidos los legales, estatutarios, reglamentarios o contractuales, deberían tenerse en cuenta cuando: a) se desarrollan políticas y procedimientos de SI; b) se diseñan, aplican o modifican los controles de SI; c) se clasifica la información y otros activos asociados como parte del proceso para establecer requisitos de SI para necesidades internas o acuerdos con proveedores;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	d) se realizan evaluaciones de riesgos de SI y se determinan las actividades de tratamiento de riesgos de SI; e) se determinan los procesos junto con las funciones y responsabilidades relacionadas con la SI; f) se determinan los requisitos contractuales de los proveedores pertinentes para la organización y el alcance del suministro de productos y servicios. **Legislación y regulaciones** La organización debería: a) identificar toda la legislación y las normativas pertinentes a la SI de la organización para conocer los requisitos de su tipo de negocio; b) tomar en consideración el cumplimiento en todos los países pertinentes, si la organización: - realiza negocios en otros países; - utiliza productos y servicios de otros países en los que las leyes y normativas pueden afectar a la organización; - transfiere información a través de fronteras jurisdiccionales donde las leyes y reglamentos pueden afectar a la organización; c) revisar periódicamente la legislación y el reglamento identificados a fin de mantenerse al día con los cambios e identificar la nueva legislación; d) definir y documentar los procesos específicos y las responsabilidades individuales para cumplir con estos requisitos. **Cifrado** El campo del cifrado es un área que a menudo tiene requisitos legales específicos. Se debería tener en cuenta el cumplimiento de los acuerdos, leyes y reglamentos pertinentes relativos a los siguientes elementos: a) restricciones a la importación o exportación de hardware y software informático para la realización de funciones de cifrado; b) restricciones a la importación o exportación de hardware y software informático diseñado para que se le añadan funciones de cifrado; c) restricciones al uso del cifrado; d) métodos obligatorios o discrecionales de acceso de las autoridades de los países a la información cifrada; e) validez de firmas digitales, sellos y certificados. Se recomienda buscar asesoramiento jurídico para garantizar el cumplimiento de la legislación y las normativas pertinentes, especialmente cuando la información cifrada o las herramientas de cifrado se desplazan a través de las fronteras jurisdiccionales. **Contratos** Los requisitos contractuales relacionados con la SI deberían incluir los que se indican en: a) contratos con clientes; b) contratos con proveedores (ver 5.20); c) contratos de seguros.
OTRA INFORMACIÓN	No hay más información.

5.32. DERECHO DE PROPIEDAD INTELECTUAL

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar**	**#Legal_y_cumplimiento**	**#Gobierno_y_ecosistema**	**18.1.2**
CONTROL	La organización debería aplicar los procedimientos apropiados para proteger los derechos de propiedad intelectual.					
PROPÓSITO	Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con derechos de propiedad intelectual y uso de productos patentados.					
ORIENTACIÓN	Se deberían considerar las siguientes directrices para proteger cualquier material que pueda considerarse propiedad intelectual: a) definir y comunicar una política temática específica sobre la protección de los derechos de propiedad intelectual; b) publicar procedimientos para el cumplimiento de los derechos de propiedad intelectual					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	que definan el uso conforme del software y los productos de información; c) adquirir software solo a través de fuentes conocidas y acreditadas, para garantizar que no se infrinja el copyright; d) mantener registros de activos adecuados e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual; e) mantener evidencias y pruebas de la propiedad de licencias, manuales, etc.; f) garantizar que no se supere el número máximo de usuarios o recursos (por ejemplo, unidades de procesamiento central (CPU)) permitidos en la licencia; g) llevar a cabo revisiones para garantizar que solo se instalan el software autorizado y los productos con licencia; h) proporcionar procedimientos para mantener las condiciones de licencia adecuadas; i) proporcionar procedimientos para desechar o transferir software a otros; j) el cumplimiento de los términos y condiciones del software y de la información obtenida de redes públicas y fuentes externas; k) no duplicar, convertir a otro formato o extraer de grabaciones comerciales (video, audio) que no estén permitidas por la ley de copyright o las licencias aplicables; l) no copiar, en su totalidad o en parte, normas (por ejemplo, normas internacionales ISO/IEC), libros, artículos, informes u otros documentos, distintos de los permitidos por la ley de derechos de autor o las licencias aplicables.
OTRA INFORMACIÓN	Los derechos de propiedad intelectual incluyen los derechos de autor de software o documentos, los derechos de diseño, las marcas comerciales, las patentes y las licencias de código fuente. Los productos de software propietario se suministran normalmente bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, al limitar el uso de los productos a máquinas específicas o al limitar la copia a la creación de copias de seguridad solamente. Más información detallada sobre la gestión de activos de TI en la norma ISO/IEC 19770. Los datos se pueden obtener de fuentes externas. En general, se da el caso de que esos datos se obtengan en virtud de los términos de un acuerdo de intercambio de datos o de un instrumento jurídico similar. Dichos acuerdos de intercambio de datos deberían dejar claro qué procesamiento se permite para los datos adquiridos. También es aconsejable que se indique claramente la procedencia de los datos. Detalles sobre los acuerdos de intercambio de datos en la norma ISO/IEC 23751. Los requisitos legales, estatutarios, reglamentarios y contractuales pueden imponer restricciones a la copia de material propietario. En particular, pueden exigir que solo se pueda utilizar material desarrollado por la organización o autorizado o suministrado por el desarrollador a la organización. La infracción de los derechos de autor puede conducir a acciones legales, que pueden implicar multas y procedimientos penales. Aparte de que la organización necesita 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 de la organización.

5.33. PROTECCIÓN DE LOS REGISTROS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Proteger**	**#Legal_y_cumplimiento #Gestión_de_activos #Protección_de_la_información**	**#Defensa**	**18.1.3**
CONTROL	Los registros deberían estar protegidos de pérdidas, destrucción, falsificación, acceso no autorizado y liberación no autorizada.					
PROPÓSITO	Garantizar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales, así como de las expectativas comunitarias o sociales relacionadas con la protección y disponibilidad de los registros.					
ORIENTACIÓN	La organización debería tomar las siguientes medidas para proteger la autenticidad, fiabilidad, integridad y usabilidad de los registros, a medida que su contexto empresarial y los requisitos					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	para su gestión cambien con el tiempo: a) emitir directrices sobre el almacenamiento, la cadena de custodia y la disposición de los registros, lo que incluye la prevención de la manipulación de los registros. Estas directrices deberían estar alineadas con la política temática específica de la organización sobre gestión de registros y otros requisitos de registros; b) elaborar un programa de retención que defina los registros y el período de tiempo durante el que deberían conservarse. El sistema de almacenamiento y manipulación debería garantizar la identificación de los registros y de su período de retención, tomando en consideración la legislación o los reglamentos nacionales o regionales, así como las expectativas de la comunidad o de la sociedad, si procede. Este sistema debería permitir la destrucción apropiada de los registros después de ese período si la organización no los necesita. Al decidir sobre la protección de registros organizacionales específicos, debería considerarse la clasificación de SI correspondiente, basada en el esquema de clasificación de la organización. Los registros deberían clasificarse en tipos de registros (por ejemplo, registros contables, registros de transacciones comerciales, registros de personal, registros legales), cada uno con detalles de los períodos de retención y el tipo de medios de almacenamiento permitidos que pueden ser físicos o electrónicos. Los sistemas de almacenamiento de datos deberían elegirse de forma que los registros necesarios puedan recuperarse en un marco de tiempo y formato aceptables, dependiendo de los requisitos que se cumplan. Cuando se elijan medios de almacenamiento electrónicos, deberían establecerse procedimientos para garantizar la capacidad de acceder a los registros (tanto medios de almacenamiento como legibilidad de formato) durante todo el período de retención, a fin de proteger contra las pérdidas debidas a futuros cambios tecnológicos. Todas las claves cifradas y los programas asociados a los archivos cifrados o a las firmas digitales también deberían conservarse para permitir el descifrado de los registros durante el tiempo que se conserven (Ver 8.24). Los procedimientos de almacenamiento y manipulación deberían aplicarse de conformidad con las recomendaciones proporcionadas por los fabricantes de medios de almacenamiento. Se debería considerar la posibilidad de deterioro de los medios utilizados para el almacenamiento de registros.
OTRA INFORMACIÓN	Los registros documentan eventos o transacciones individuales o pueden formar agregaciones diseñadas para documentar procesos, actividades o funciones de trabajo. Éstos constituyen pruebas de la actividad empresarial y de los activos de información. Cualquier conjunto de información, independientemente de su estructura o formulario, se puede administrar como un registro. Esto incluye información en forma de documento, recopilación de datos u otros tipos de información digital o analógica que se crean, capturan y gestionan en el curso de la actividad empresarial. En la gestión de registros, los metadatos son datos que describen el contexto, el contenido y la estructura de los registros, así como su gestión a lo largo del tiempo. Los metadatos son un componente esencial de cualquier documento. Puede ser necesario conservar algunos registros de forma segura para cumplir con los requisitos legales, estatutarios, reglamentarios o contractuales, así como para apoyar las actividades empresariales esenciales. La legislación nacional puede establecer el período de tiempo y el contenido de los datos para la conservación de la información. Más información sobre la gestión de documentos en la norma ISO 15489.

5.34. PRIVACIDAD Y PROTECCIÓN DE LA IIP

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Corrección**	**#Confidencialidad #Integridad #Disponibilidad**	**#Identifivcar #Proteger**	**#Proteccion_de_la_información #Legal_y_cumplimiento**	**#Defensa**	**18.1.4**
CONTROL	La organización debería identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.					
PROPÓSITO	Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de SI de la protección de la IIP.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ORIENTACIÓN	La organización debería establecer y comunicar una política específica sobre privacidad y protección de la IIP a todas las partes interesadas pertinentes. La organización debería desarrollar e implementar procedimientos para la preservación de la privacidad y la protección de la IIP. Estos procedimientos deberían comunicarse a todas las partes interesadas pertinentes que participen en el tratamiento de la IIP. El cumplimiento de estos procedimientos y de toda la legislación y normativa pertinente relativa a la preservación de la privacidad y la protección de la IIP requiere funciones, responsabilidades y controles apropiados. A menudo, esto se consigue mejor con el nombramiento de una persona responsable, como un funcionario de privacidad, que debería proporcionar guía al personal, proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que deberían seguirse. La responsabilidad de la manipulación de la IIP debería abordarse tomando en consideración la legislación y los reglamentos pertinentes. Deberían aplicarse medidas técnicas y organizativas apropiadas para proteger la IIP.
OTRA INFORMACIÓN	Varios países han introducido una legislación que controla la recolección, el tratamiento, la transmisión y la eliminación de la IIP. Dependiendo de la legislación nacional respectiva, tales controles pueden imponer obligaciones a los que recolectan, procesan y difunden la IIP y también pueden restringir la autoridad para transferir la IIP a otros países. Un marco de alto nivel para la protección de la IIP en los sistemas de TIC en la norma ISO/IEC 29100. Más información sobre los sistemas de gestión de la información sobre la privacidad en la norma ISO/IEC 27701. Información específica sobre la gestión de la información de privacidad para las nubes públicas que actúan como procesadores IIP en la norma ISO/IEC 27018. Directrices para la evaluación del impacto en la privacidad (PIA) y un ejemplo de la estructura y el contenido de un informe de PIA en la norma ISO/IEC 29134 proporciona. En comparación con la norma ISO/IEC 27005, se centra en el procesamiento de la IIP y es pertinente para las organizaciones que procesan IIP. Esto puede ayudar a identificar riesgos de privacidad y posibles mitigaciones para reducir estos riesgos a niveles aceptables.

5.35. REVISIÓN INDEPENDIENTE DE LA SI

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Correctivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Protegerr**	**#Seguridad_de_la_información**	**#Gobierno_y_ecosistema**	**18.2.1**
CONTROL	El enfoque de la organización para gestionar la SI y su implementación, incluidas las personas, los procesos y las tecnologías, debería revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.					
PROPÓSITO	Garantizar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la SI.					
ORIENTACIÓN	La organización debería tener procesos para realizar revisiones independientes. La dirección debería planificar e iniciar revisiones independientes periódicas. Las revisiones deberían incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la SI, lo que incluye la política de SI, las políticas de temas específicos y otros controles. Dichas revisiones deberían ser llevadas a cabo por personas independientes del área revisada (por ejemplo, la función de auditoría interna, un gestor independiente o una organización externa especializada en dichas revisiones). Las personas que lleven a cabo estas revisiones deberían tener la competencia adecuada. La persona que lleve a cabo las revisiones no debería estar en la línea de autoridad para garantizar que tenga la independencia necesaria para realizar una evaluación. Los resultados de las revisiones independientes deberían comunicarse a los directivos que las iniciaron y, en su caso, a la alta dirección. Estos documentos deberían conservarse. Si las revisiones independientes identifican que el enfoque y la implementación de la organización para administrar la SI son inadecuados (por ejemplo, los objetivos y requisitos documentados no se cumplen o no se ajustan con la dirección de SI indicada en la política de SI y las políticas de temas específicos (ver 5.1)), la dirección debería iniciar acciones correctivas. Además de las revisiones periódicas independientes, la organización debería considerar la posibilidad de realizar revisiones independientes cuando: a) leyes y reglamentos que afectan al cambio de organización; b) se producen incidentes significativos;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	c) la organización inicia un nuevo negocio o cambia un negocio actual; d) la organización comienza a utilizar un nuevo producto o servicio o cambia el uso de un producto o servicio actual; e) la organización cambia significativamente los controles y procedimientos de SI.
OTRA INFORMACIÓN	Guía para llevar a cabo revisiones independientes en las normas ISO/IEC 27007 e ISO/IEC TS 27008.

5.36. CUMPLIMIENTO DE POLÍTICAS, REGLAS Y NORMAS DE SI

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Proteger**	**#Legal_y_cumplimiento #Seguridad_de_la_información**	**#Gobierno_y_ecosistema**	**18.2.2 18.2.3**
CONTROL	El cumplimiento de la política de SI de la organización, las políticas, las reglas y los estándares específicos de cada tema deberían revisarse periódicamente.					
PROPÓSITO	Garantizar que la SI se implementa y opera de acuerdo con la política de SI de la organización, las políticas, reglas y normas específicas de cada tema.					
ORIENTACIÓN	Los administradores, los propietarios de servicios, productos o información deberían identificar cómo revisar que se cumplen los requisitos de SI definidos en la política de SI, las políticas específicas de cada tema, las reglas, las normas y otras regulaciones que sean aplicables. Se deberían considerar las herramientas automáticas de medición y elaboración de informes para una revisión periódica eficaz. Si se encuentra alguna no conformidad como resultado de la revisión, los administradores deben: a) identificar las causas de la no conformidad; b) evaluar la necesidad de medidas correctivas para lograr la conformidad; c) implementar las acciones correctivas adecuadas; d) revisar las medidas correctivas adoptadas para verificar su eficacia e identificar deficiencias o debilidades. Se deberían registrar los resultados de las revisiones y acciones correctivas llevadas a cabo por los gerentes, los propietarios de servicios, productos o información y se deberían conservar estos documentos. Los administradores deberían informar los resultados a las personas que realizan revisiones independientes (ver 5.35) cuando se lleve a cabo una revisión independiente en el área de su responsabilidad. Las acciones correctivas deberían completarse de manera oportuna, según corresponda al riesgo. Si no se completa en la próxima revisión programada, los progresos deberían abordarse al menos en esa revisión.					
OTRA INFORMACIÓN	El seguimiento operativo del uso del sistema se trata en 8.15, 8.16 y 8.17.					

5.37. PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#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_la_identidad_y_del_acceso #Gestión_de_las_amenazas_y_de_la_vulnerabilidad #Continuidad #Gestión_de_eventos_de_SI**	**#Gobierno_y_ecosistema #Protección #Defensa**	**12.1.1**
CONTROL	Los procedimientos operativos para las instalaciones de procesamiento de la información deberían estar documentados y disponibles para el personal que los necesite.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

PROPÓSITO	Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.
ORIENTACIÓN	Se deberían preparar los procedimientos documentados para las actividades operacionales de la organización asociadas con la SI, por ejemplo, cuando la actividad: a) necesite ser realizada de la misma manera por muchas personas; b) se realiza en raras ocasiones y la siguiente vez que se realiza, es probable que se haya olvidado el procedimiento; c) es nueva y presenta un riesgo si no se realiza correctamente; d) la actividad de va a al nuevo personal. Los procedimientos operativos deberían especificar: a) personas responsables; b) instalación y configuración seguras de los sistemas; c) procesamiento y manejo de la información, tanto automatizada como manual; d) respaldo (ver 8.13) y resiliencia; e) requisitos de programación, incluidas las interdependencias con otros sistemas; f) instrucciones para gestionar errores u otras condiciones excepcionales (por ejemplo, restricciones en el uso de programas utilitarios (ver 8.18)), que pueden surgir durante la ejecución del trabajo; g) contactos de asistencia y escalada, incluidos contactos de asistencia externa en caso de dificultades técnicas u operativas inesperadas; h) instrucciones de manipulación de los soportes de almacenamiento (ver 7.10 y 7.14); i) procedimientos de reinicio y recuperación del sistema para su uso en caso de; j) gestión de la información del registro de auditoría y del registro del sistema (ver 8.15 y 8.17) y de los sistemas de monitoreo de video (ver 7.4); k) procedimientos de monitoreo como la capacidad, el rendimiento y la seguridad (ver 8.6 y 8.16); l) instrucciones de mantenimiento. Los procedimientos operativos documentados deberían revisarse y actualizarse cuando sea necesario. Se deberían autorizar los cambios en los procedimientos operativos documentados. Cuando sea técnicamente factible, los sistemas de información deberían gestionarse de manera coherente, al utilizar los mismos procedimientos, herramientas y servicios públicos.
OTRA INFORMACIÓN	No hay más información.

6. CONTROLES DE PERSONAS

6.1. SELECCIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_los_recursos_humanos**	**#Gobierno_y_ecosistema**	**7.1.1**
CONTROL	Las verificaciones de los antecedentes de todos los candidatos a convertirse en personal deberían llevarse a cabo antes de incorporarse a la organización y de forma continuada, tomando en consideración las leyes, los reglamentos y la ética aplicables y ser proporcionales a los requisitos de la empresa, la clasificación de la información a la que se va a acceder y los riesgos percibidos.					
PROPÓSITO	Garantizar que todo el personal es elegible y adecuado para las funciones para las que se considera y que sigue siendo elegible y adecuado durante su empleo.					
ORIENTACIÓN	Se debería realizar un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. Cuando estas personas se contraten a través de proveedores de servicios, los requisitos de selección se deberían incluir en los acuerdos contractuales entre la organización y los proveedores. La información sobre todos los candidatos que se consideren para puestos dentro de la organización debería ser recolectada y manejada tomando en consideración cualquier legislación apropiada existente en la jurisdicción pertinente. En algunas jurisdicciones, la organización puede ser legalmente requerida para informar a los candidatos previamente sobre las actividades de selección. La verificación debería tener en cuenta toda la legislación pertinente en materia de privacidad, protección de la IIP y basada en el empleo y, cuando lo permita, debería incluir: a) disponibilidad de referencias satisfactorias (por ejemplo, referencias comerciales y					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	personales); b) verificación (para la integridad y exactitud) del currículum vitae del solicitante; c) confirmación de las calificaciones académicas y profesionales declaradas; d) verificación independiente de la identidad (por ejemplo, pasaporte u otro documento aceptable expedido por las autoridades competentes); e) verificación más detallada, como la revisión de crédito o la revisión de registros criminales si el candidato asume un papel crítico. Cuando se contrata a un individuo para una función específica de SI, la organización debería asegurarse de que el candidato: a) tenga la competencia necesaria para desempeñar el papel de seguridad; b) se pueda confiar en él para asumir el rol, especialmente si el rol es crítico para la organización. Cuando un puesto de trabajo ya sea en el momento del nombramiento inicial o de la promoción, implique que la persona tenga acceso a instalaciones de procesamiento de información y, en especial, si éstas implican el manejo de información confidencial (por ejemplo, información financiera, personal o médica), la organización también debería considerar la posibilidad de realizar verificaciones adicionales más detalladas. Los procedimientos deberían definir criterios y limitaciones para las revisiones de verificación (por ejemplo, quién puede seleccionar a las personas y cómo, cuándo y por qué se llevan a cabo las revisiones de verificación). En situaciones en las que la verificación no se puede completar de forma oportuna, se deberían implementar controles atenuantes hasta que se haya terminado la revisión, por ejemplo: a) retraso en la incorporación; b) retraso en la entrega de activos corporativos; c) incorporación con acceso reducido; d) terminación del empleo. Los controles de verificación deberían repetirse periódicamente para confirmar la idoneidad continua del personal, dependiendo de la criticidad de la función de una persona.
OTRA INFORMACIÓN	No hay más información.

6.2. CONDICIONES DEL EMPLEO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_los_recursos_humanos**	**#Gobierno_y_ecosistema**	**7.1.2**
CONTROL	Los acuerdos contractuales de empleo deberían indicar las responsabilidades del personal y de la organización en materia de SI.					
PROPÓSITO	Garantizar que el personal comprenda sus responsabilidades de SI para las funciones para las que se consideran.					
ORIENTACIÓN	Las obligaciones contractuales para el personal deberían tener en cuenta la política de SI de la organización y las políticas pertinentes relativas a temas específicos. Además, se pueden aclarar y precisar los siguientes puntos: a) acuerdos de confidencialidad o no divulgación que el personal al que se dé acceso a información confidencial debería firmar antes de que se le dé acceso a la información y otros activos asociados (ver 6.6); b) responsabilidades y derechos legales (por ejemplo, con respecto a las leyes de derechos de autor o la legislación sobre protección de datos (ver 5.32 y 5.34)); c) responsabilidades para la clasificación de la información y la gestión de la información de la organización y otros activos asociados, instalaciones de procesamiento de información y servicios de información gestionados por el personal (ver 5.9 al 5.13); d) responsabilidades para el manejo de la información recibida de las partes interesadas; e) acciones a tomar si el personal ignora los requisitos de seguridad de la organización (ver 6.4). Las funciones y responsabilidades de SI deberían comunicarse a los candidatos durante el proceso de precontratación. La organización debería asegurarse de que el personal acepte los términos y condiciones					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	relativos a la SI. Estos términos y condiciones deberían ser apropiados a la naturaleza y el grado de acceso que tengan a los activos de la organización asociados con los sistemas y servicios de información. Los términos y condiciones relativos a la SI deberían revisarse cuando cambien las leyes, reglamentos, la política de SI o las políticas específicas de cada tema. Las responsabilidades contenidas en las condiciones de empleo deberían continuar durante un período determinado después del final del empleo (ver 6.5).
OTRA INFORMACIÓN	Se puede utilizar un código de conducta para las responsabilidades de SI del personal del estado en relación con la confidencialidad, la protección de la IIP, la ética, el uso apropiado de la información de la organización y otros activos asociados, así como las prácticas de reputación esperadas por la organización. Una parte externa, con la que el personal del proveedor está asociado, puede estar obligado a celebrar acuerdos contractuales en nombre de la persona contratada. Si la organización no es una entidad legal y no tiene empleados, el equivalente del acuerdo contractual y los términos y condiciones pueden considerarse de acuerdo con la directriz de este control.

6.3. SENSIBILIZACIÓN, EDUCACIÓN Y FORMACIÓN EN MATERIA DE SI

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_los_recursos_humanos**	**#Gobierno_y_ecosistema**	**7.2.2**
CONTROL	El personal de la organización y las partes interesadas pertinentes deberían recibir una sensibilización, educación y formación adecuadas en materia de SI, así como actualizaciones periódicas de la política de SI de la organización y de las políticas y procedimientos específicos, según sea pertinente para su función laboral.					
PROPÓSITO	Garantizar que el personal y las partes interesadas pertinentes conozcan y cumplan con sus responsabilidades en materia de SI.					
ORIENTACIÓN	**General** Se debería establecer un programa de sensibilización, educación y formación en materia de SI en consonancia con la política de SI, las políticas específicas de cada tema y los procedimientos pertinentes en materia de SI, tomando en consideración la información de la organización que se debería proteger y los controles de SI que se han aplicado para protegerla. La sensibilización, la educación y la formación en materia de SI deberían tener lugar periódicamente. La sensibilización inicial, la educación y la capacitación pueden aplicarse al nuevo personal y a quienes se transfieren a nuevos puestos o funciones con requisitos de SI sustancialmente diferentes. La comprensión del personal debería evaluarse al final de una actividad de sensibilización, educación o capacitación para poner a prueba la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y capacitación. **Sensibilización** Un programa de concienciación sobre la SI debería tener por objeto sensibilizar al personal acerca de sus responsabilidades en materia de SI y de los medios por los que se han cumplido dichas responsabilidades. El programa de sensibilización debería planificarse tomando en consideración las funciones del personal de la organización, incluido el personal interno y externo (por ejemplo, consultores externos, personal de proveedores). Las actividades del programa de sensibilización deberían programarse con el tiempo, preferiblemente regularmente, de modo que las actividades se repitan y abarquen al nuevo personal. También debería construirse sobre la base de las lecciones aprendidas de los incidentes de SI. El programa de sensibilización debería incluir una norma de actividades de sensibilización a través de canales físicos o virtuales apropiados, como campañas, folletos, carteles, boletines, sitios web, sesiones de información, sesiones informativas, módulos de e-learning y correos electrónicos. El conocimiento de la SI debería abarcar aspectos generales como: a) compromiso de la administración con la SI en toda la organización; b) familiaridad y necesidades de cumplimiento con respecto a las normas y obligaciones de SI aplicables, tomando en consideración la política de SI y las políticas, normas,					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	leyes, estatutos, reglamentos específicos de cada tema, contratos y acuerdos; c) responsabilidad personal por las propias acciones e inacciones y responsabilidades generales para asegurar o proteger la información que pertenece a la organización y a las partes interesadas; d) procedimientos básicos de SI (por ejemplo, informes de eventos de SI (ver 6.8)) y controles de referencia (por ejemplo, seguridad mediante contraseña (ver 5.17)); e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre cuestiones de SI, incluidos otros materiales de sensibilización sobre SI. **Educación y formación** La organización debería identificar, preparar e implementar un plan de capacitación apropiado para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y experiencia específicos. Los equipos técnicos deberían tener las habilidades necesarias para configurar y mantener el nivel de seguridad necesario para dispositivos, sistemas, aplicaciones y servicios. Si faltan habilidades, la organización debería tomar medidas para obtenerlas. El programa de educación y formación debería contemplar diferentes formas (por ejemplo, conferencias o autoaprendizaje, ser asesorado por personal experto o consultores (formación en el puesto de trabajo), rotar a los miembros del personal para que sigan diferentes actividades, contratar a personas ya capacitadas y contratar consultores). Puede utilizarse diferentes medios de entrega, que incluyen clases, aprendizaje a distancia, basado en la web, autodidacta y otros. El personal técnico debería mantener sus conocimientos actualizados al suscribirse a boletines y revistas o asistiendo a conferencias y eventos dirigidos a la mejora técnica y profesional.
OTRA INFORMACIÓN	Al redactar un programa de sensibilización, es importante no solo centrarse en el «qué» y el «cómo», sino también en el «por qué», cuando sea posible. Es importante que el personal comprenda el objetivo de la SI y el efecto potencial, positivo y negativo, en la organización de su propio comportamiento. La sensibilización, la educación y la formación en materia de SI pueden formar parte de otras actividades, como la gestión general de la información, las TIC, la seguridad, la privacidad o la formación en materia de seguridad.

6.4. PROCESO DISCIPLINARIO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Corrección	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger #Responder**	**#Seguridad_de_los_recursos_humanos**	**#Gobierno_y_ecosistema**	**7.2.3**
CONTROL	Se debería formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de SI.					
PROPÓSITO	Garantizar que el personal y otras partes interesadas comprendan las consecuencias de la violación de la política de SI, para disuadir y tratar adecuadamente al personal y otras partes interesadas pertinentes que hayan cometido la violación.					
ORIENTACIÓN	El proceso disciplinario no debería iniciarse sin una verificación previa de que se ha producido una violación de la política de SI (ver 5.28). El proceso disciplinario formal debería proporcionar una respuesta graduada que tome en consideración factores tales como: a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad de la violación y sus consecuencias; b) si el delito fue intencional (malicioso) o no intencional (accidental); c) tanto si se trata de una primera infracción como de una reincidencia; d) si el infractor estaba debidamente formado o no. La respuesta debería tener en cuenta los requisitos legales, reglamentarios, contractuales y organizacionales pertinentes, así como otros factores según sea necesario. El proceso disciplinario también debería utilizarse como elemento disuasorio para evitar que el personal y otras partes interesadas pertinentes infrinjan la política de SI, las políticas específicas del tema y los procedimientos de SI. Las infracciones deliberadas de la política de SI pueden requerir acciones inmediatas.					
OTRA IN-	Siempre que sea posible, la identidad de las personas sujetas a medidas disciplinarias					

FORMACIÓN	debería protegerse de conformidad con los requisitos aplicables. Si las personas demuestran un comportamiento excelente en materia de SI, se les puede recompensar para promover la SI y fomentar el buen comportamiento.

6.5. RESPONSABILIDADES TRAS EL TERMINO O EL CAMBIO DE EMPLEO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_los_recursos_humanos #Gestión_de_activos**	**#Gobierno_y_ecosistema**	**7.3.1**
CONTROL	Las responsabilidades y deberes de SI que siguen siendo válidos después de la terminación o el cambio de empleo deberían definirse, aplicarse y comunicarse 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 administrar la terminación o el cambio de empleo debería definir qué responsabilidades y deberes de SI deberían seguir siendo válidos después de la terminación o el cambio. Esto puede incluir la confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos, así como las responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (ver 6.6). Las responsabilidades y deberes que siguen siendo válidos después de la terminación del empleo o del contrato deberían figurar en los términos y condiciones de empleo del individuo (ver 6.2), contrato o acuerdo. Otros contratos o acuerdos que continúen por un período definido después del final del empleo de la persona también pueden contener responsabilidades de SI. Los cambios de responsabilidad o de empleo deberían gestionarse como la terminación de la responsabilidad o del empleo actual, combinado con la iniciación de la nueva responsabilidad o empleo. Las funciones y responsabilidades de SI que tenga cualquier persona que abandone o cambie las funciones del trabajo deberían identificarse y transferirse a otra persona. Debería establecerse un proceso para la comunicación de los cambios y de los procedimientos operativos al personal, a otras partes interesadas y a las personas de contacto pertinentes (por ejemplo, a clientes y proveedores). El proceso para la terminación o el cambio de empleo también debería aplicarse al personal externo (es decir, a los proveedores) cuando se produce una terminación del personal, el contrato o el trabajo con la organización o cuando hay un cambio de trabajo dentro de la organización.					
OTRA INFORMACIÓN	En muchas organizaciones, la función de recursos humanos es generalmente responsable del proceso general de terminación y trabaja junto con el gerente supervisor de la persona en transición para administrar los aspectos de SI de los procedimientos pertinentes. En el caso del personal proporcionado a través de una parte externa (por ejemplo, a través de un proveedor), este proceso de terminación es llevado a cabo por la parte externa de acuerdo con el contrato entre la organización y la parte externa.					

6.6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad**	**#Proteger**	**#Seguridad_de_los_recursos_humanos #Protección_de_la_información #Relaciones_con_los_proveedores**	**#Gobierno_y_ecosistema**	**13.2.4**
CONTROL	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deberían ser identificados, documentados,					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	revisados y firmados regularmente por el personal y otras partes interesadas pertinentes.
PROPÓSITO	Mantener la confidencialidad de la información accesible por el personal o terceros.
ORIENTACIÓN	Los acuerdos de confidencialidad o no divulgación deberían abordar el requisito de proteger la información confidencial usando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. Sobre la base de los requisitos de SI, los términos de los acuerdos deberían determinarse tomando en consideración el tipo de información que se manejará, su nivel de clasificación, su uso y el acceso permitido por la otra parte. Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se deberían considerar: a) una definición de la información que se va a proteger (por ejemplo, información confidencial); b) la duración prevista de un acuerdo, incluidos los casos en que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté disponible públicamente; c) las acciones necesarias cuando se termina un acuerdo; d) las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada; e) la propiedad de la información, los secretos comerciales y la propiedad intelectual y cómo se relaciona con la protección de la información confidencial; f) el uso permitido de información confidencial y los derechos del signatario a utilizar la información; g) el derecho a auditar y supervisar actividades que impliquen información confidencial en circunstancias muy sensibles; h) el proceso para la notificación y notificación de revelación no autorizada o fuga de información confidencial; i) los términos de la información que se devolverá o destruirá en el momento de la terminación del acuerdo; j) las medidas previstas en caso de incumplimiento del acuerdo. La organización debería tener en cuenta el cumplimiento de los acuerdos de confidencialidad y no divulgación de la jurisdicción a la que se aplican (ver 5.31, 5.32, 5.33 y 5.34). Los requisitos para los acuerdos de confidencialidad y no divulgación deberían revisarse periódicamente y cuando se produzcan cambios que influyan en estos requisitos.
OTRA INFORMACIÓN	Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad de proteger, utilizar y divulgar la información de una manera responsable y autorizada.

6.7. TRABAJO REMOTO

	Tipo de Control	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión de activos #Protección_de_la_información #Seguridad_física #Seguridad_del_sistema_y_de_la_red**	**#Protección**	**6.2.2**
CONTROL	Deberían implementarse medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.					
PROPÓSITO	Garantizar la SI cuando el personal trabaja de forma remota.					
ORIENTACIÓN	El trabajo a distancia ocurre siempre que el personal de la organización trabaja desde un lugar fuera de las instalaciones de la organización, al acceder a información ya sea en papel o electrónicamente a través de equipos de TIC. Los entornos de trabajo remoto incluyen los denominados “teletrabajo”, “trabajo a distancia”, “trabajo flexible”, “entornos de trabajo virtuales” y “mantenimiento remoto”. NOTA Es posible que no todas las recomendaciones de esta guía se puedan aplicar debido a la legislación local y a las regulaciones en diferentes jurisdicciones. Las organizaciones que permiten actividades de trabajo remoto deberían emitir una política específica sobre trabajo remoto que defina las condiciones y restricciones pertinentes. Cuando se considere aplicable, se deberían considerar los siguientes asuntos: a) la seguridad física existente o propuesta del lugar de trabajo remoto, tomando en					

	consideración la seguridad física de la ubicación y el entorno local, incluidas las diferentes jurisdicciones en las que se encuentra el personal; b) las reglas y mecanismos de seguridad para el entorno físico remoto, como archivadores bloqueables, transporte seguro entre ubicaciones y reglas para acceso remoto, escritorio transparente, impresión y eliminación de información y otros activos asociados, e informes de eventos de SI (ver 6.8); c) los entornos de trabajo remotos físicos esperados; d) los requisitos de seguridad de las comunicaciones, tomando en consideración la necesidad de acceso remoto a los sistemas de la organización, la sensibilidad de la información a la que se accede y se transmite a través del enlace de comunicaciones y la sensibilidad de los sistemas y aplicaciones; e) el uso de acceso remoto, como el acceso a escritorios virtuales, que admite el procesamiento y almacenamiento de información en equipos de propiedad privada; f) la amenaza del acceso no autorizado a la información o los recursos de otras personas en el lugar de trabajo remoto (por ejemplo, familiares y amigos); g) la amenaza del acceso no autorizado a la información o a los recursos de otras personas en lugares públicos; h) el uso de redes domésticas y redes públicas, así como los requisitos o restricciones en la configuración de servicios de red inalámbrica; i) el uso de medidas de seguridad, como firewalls y protección contra malware; j) los mecanismos seguros para desplegar e inicializar sistemas de forma remota; k) los mecanismos seguros para la autenticación y la habilitación de privilegios de acceso tomando en consideración la vulnerabilidad de los mecanismos de autenticación de factor único en los que se permite el acceso remoto a la red de la empresa. Las directrices y medidas que se deberían considerarse deberían incluir: a) el suministro de equipo y mobiliario de almacenamiento adecuados para las actividades de trabajo a distancia, cuando no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización; b) una definición del trabajo permitido, la clasificación de la información que se puede mantener y los sistemas y servicios internos a los que está autorizado el trabajador remoto; c) la formación de los que trabajan a distancia y de los que prestan apoyo. Esto debería incluir cómo llevar a cabo el negocio de forma segura mientras trabaja de forma remota; d) el suministro de equipos de comunicación adecuados, incluidos métodos para garantizar el acceso remoto, como requisitos sobre bloqueos de pantalla del dispositivo y temporizadores de inactividad; la activación del seguimiento de la ubicación del dispositivo; la instalación de capacidades de borrado remoto; e) la seguridad física; f) las normas y directrices sobre el acceso de la familia y los visitantes al equipo y a la información; g) la prestación de asistencia y mantenimiento de hardware y software; h) la provisión de seguros; i) los procedimientos de respaldo y continuidad del negocio; j) auditoría y vigilancia de la seguridad; k) la revocación de la autoridad y los derechos de acceso y la devolución del equipo cuando se terminan las actividades de trabajo remoto.
OTRA INFORMACIÓN	No hay más información.

6.8. INFORMES DE EVENTOS DE SI

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Detectivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Detectar**	**#Gestión_de_eventos_de_SI**	**#Defensa**	**16.1.2 16.1.3**
CONTROL	La organización debería proporcionar un mecanismo para que el personal informe sobre los eventos de SI observados o sospechados a través de los canales apropiados de manera oportuna.					
PROPÓSITO	Apoyar la notificación oportuna, coherente y eficaz de los eventos de SI que pueden ser identificados por el personal.					
ORIENTACIÓN	Todo el personal y los usuarios deberían ser conscientes de su responsabilidad de informar sobre los eventos de SI lo antes posible para evitar o minimizar el efecto de los incidentes					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	de SI. También deberían tener en cuenta el procedimiento para informar sobre los eventos de SI y el punto de contacto al que deberían notificarse los eventos. El mecanismo de presentación de informes debería ser lo más fácil, accesible y disponible posible. Los eventos de SI incluyen incidentes, violaciones y vulnerabilidades. Entre las situaciones que se deberían tener en cuenta para los informes de eventos de SI se incluyen: a) controles de SI ineficaces; b) incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información; c) errores humanos; d) incumplimiento de la política de SI, las políticas de temas específicos o las normas aplicables; e) violaciones de las medidas de seguridad física; f) cambios del sistema que no han pasado por el proceso de gestión de cambios; g) fallas de funcionamiento u otro comportamiento anómalo del software o hardware en el sistema; h) violaciones de acceso; i) vulnerabilidades; j) sospecha de infección de malware. Se le debería aconsejar al personal y a los usuarios que no intenten probar posibles vulnerabilidades de SI. Las vulnerabilidades de prueba se pueden interpretar como un posible mal uso del sistema y también pueden causar daños al sistema o servicio de información y pueden dañar u ocultar las pruebas digitales. En última instancia, esto puede resultar en responsabilidad legal para el individuo que realiza la prueba.
OTRA INFORMACIÓN	Información adicional en la norma ISO/IEC 27035.

7. CONTROLES FÍSICOS

7.1. PERÍMETROS DE SEGURIDAD FÍSICA

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física**	**#Protección**	**11.1.1**
CONTROL	Los perímetros de seguridad deberían definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.					
PROPÓSITO	Evitar 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 considerarse e implementarse cuando sea apropiado para los perímetros de seguridad física: a) definir los perímetros de seguridad y el emplazamiento y la fuerza de cada uno de los perímetros de acuerdo con los requisitos de SI relacionados con los activos dentro del perímetro; b) tener perímetros físicamente sólidos para un edificio o sitio que contenga instalaciones de procesamiento de información (es decir, no debería haber espacios en el perímetro o áreas donde pueda ocurrir fácilmente una violación). Los techos exteriores, las paredes, los techos y el suelo del emplazamiento 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, barras, alarmas, cerraduras). Las puertas y ventanas deberían bloquearse cuando no estén vigiladas y se debería considerar la protección externa para las ventanas, especialmente a nivel del suelo; también deberían considerarse los puntos de ventilación; c) tener alarmas, realizar monitoreo y prueba de todas las puertas contra incendios en un perímetro de seguridad junto con las paredes para establecer el nivel requerido de resistencia de acuerdo con estándares adecuados. Deberían funcionar de forma segura.					
OTRA IN-	La protección física se puede lograr creando una o más barreras físicas alrededor de las					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

FORMACIÓN	instalaciones de la organización y las instalaciones de procesamiento de información. Una zona segura puede ser una oficina con cerradura o varias salas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarias barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. La organización debería considerar la posibilidad de adoptar medidas de seguridad física que puedan fortalecerse durante situaciones de mayor amenaza.

7.2. ENTRADA FÍSICA

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física #Gestión_de_la_identidad_y_del_acceso**	**#Protección**	**11.1.2 11.1.6**
CONTROL	Las áreas seguras deberían protegerse mediante controles de entrada y puntos de acceso adecuados.					
PROPÓSITO	Garantizar que solo 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 personas no autorizadas puedan entrar en las instalaciones, deberían controlarse y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. Se deberían tomar en consideración las siguientes directrices: a) restringir el acceso a los sitios y edificios solo al personal autorizado. El proceso de gestión de los derechos de acceso a las áreas físicas debería incluir la provisión, revisión periódica, actualización y revocación de autorizaciones (ver 5.18); b) mantener y supervisar de forma segura un libro de registro físico o un registro de auditoría electrónico de todos los accesos y proteger todos los registros (ver 5.33) y la información confidencial de autenticación; c) establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Para el acceso a zonas sensibles deberían considerarse puertas de seguridad dobles; d) establecer un área de recepción supervisada por el personal u otros medios para controlar el acceso físico al sitio o al edificio; e) inspeccionar y examinar las pertenencias personales del personal y de las partes interesadas en el momento de la entrada y salida; NOTA Pueden existir legislaciones y normativas locales sobre la posibilidad de inspeccionar los objetos personales. f) requerir a todo el personal y a las partes interesadas que lleven algún tipo de identificación visible y que notifiquen inmediatamente al personal de seguridad si se encuentran con visitantes no escoltados y alguien que no lleve identificación visible. Deberían considerarse insignias fácilmente distinguibles para identificar mejor a los empleados, proveedores y visitantes permanentes; g) conceder al personal del proveedor acceso restringido a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario. Este acceso debería autorizarse y supervisarse; h) prestar especial atención a la seguridad del acceso físico en el caso de los edificios que tienen activos para múltiples organizaciones; i) diseñar medidas de seguridad física para que puedan reforzarse cuando aumente la probabilidad de incidentes físicos; j) asegurar otros puntos de entrada, como salidas de emergencia, frente a accesos no autorizados; k) configurar un proceso de gestión de claves para garantizar la gestión de las claves físicas o la información de autenticación (por ejemplo, códigos de bloqueo, bloqueos combinados a oficinas, salas e instalaciones como armarios de llaves) y garantizar un libro					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	de registro o una auditoría de claves anual y el acceso a la información física las claves o la información de autenticación se controlan (ver 5.17 para obtener más información sobre la autenticación). **Visitantes** Se deberían tomar en consideración las siguientes directrices: a) autenticar la identidad de los visitantes por un medio apropiado; b) registrar la fecha y hora de entrada y salida de los visitantes; c) conceder acceso únicamente a los visitantes con 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. Áreas de entrega y carga y material entrante Se deberían tomar en consideración las siguientes directrices: a) restringir el acceso a las zonas de entrega y carga desde fuera del edificio al personal identificado y autorizado; b) diseñar las áreas de entrega y carga para que las entregas puedan cargarse y descargarse sin que el personal de entrega tenga acceso no autorizado a otras partes del edificio; c) asegurar las puertas externas de las zonas de entrega y carga cuando se abren las puertas a zonas restringidas; d) inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de trasladarlas de las zonas de entrega y carga; e) registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos (ver 5.9 y 7.10) en el momento de la entrada en el emplazamiento; f) separar físicamente los envíos entrantes y salientes, siempre que sea posible; g) inspección de las entregas entrantes para comprobar si hay indicios de manipulación en el camino. Si se descubre la manipulación, se debería informar inmediatamente al personal de seguridad.
OTRA INFORMACIÓN	No hay más información.

7.3. PROTECCIÓN DE OFICINAS, SALAS E INSTALACIONES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física #Gestión_de_activos**	**#Protección**	**11.1.3**
CONTROL	Se debería diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.					
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	Se deberían considerar las siguientes directrices para asegurar oficinas, salas e instalaciones: a) ubicar adecuadamente las instalaciones críticas para evitar el acceso del público; b) cuando sea aplicable, garantizar que los edificios sean discretos y dar una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, identificando la presencia de actividades de procesamiento de información; c) configurar las funciones para evitar que la información confidencial o las actividades sean visibles y audibles desde el exterior. El blindaje electromagnético también debería considerarse apropiado; d) no tener directorios, ORIENTACIÓN telefónicas internas y mapas accesibles en línea que identifiquen ubicaciones de instalaciones de procesamiento de información confidencial fácilmente disponibles para cualquier persona no autorizada.					
OTRA INFORMACIÓN	No hay más información.					

7.4. MONITOREO DE SEGURIDAD FÍSICA

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección	Nuevo
CONTROL	Las instalaciones deberían ser vigiladas continuamente para detectar el acceso físico no autorizado.					
PROPÓSITO	Detectar y disuadir el acceso físico no autorizado.					
ORIENTACIÓN	Las instalaciones físicas deberían ser monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas de intrusos, sistemas de monitoreo de video como la televisión de circuito cerrado y software de gestión de información de seguridad física administrado internamente o por un proveedor de servicios de monitoreo. El acceso a los edificios que albergan sistemas críticos debería monitorearse continuamente para detectar accesos no autorizados o comportamientos sospechosos mediante: a) instalar sistemas de supervisión de video, como la televisión de circuito cerrado, para ver y grabar el acceso a áreas sensibles dentro y fuera de las instalaciones de una organización; b) instalar, de acuerdo con las normas aplicables pertinentes y probar periódicamente detectores de contacto, sonido o movimiento para activar una alarma de intrusión como: 1) detectores de contacto que activan una alarma cuando se hace o rompe un contacto en cualquier lugar donde se pueda hacer o romper un contacto (como ventanas y puertas y debajo de objetos) para su uso como alarma de emergencia; 2) detectores de movimiento basados en tecnología de infrarrojos que activan una alarma cuando un objeto pasa por su campo de visión; 3) sensores sensibles al sonido de rotura de cristal que se pueden utilizar para activar una alarma para alertar al personal de seguridad; c) utilizar estas alarmas para cubrir todas las puertas externas y ventanas accesibles. Las zonas desocupadas deberían estar con alarmas activadas en todo momento; también debería cubrirse otras zonas (por ejemplo, salas de computadores o de comunicaciones). El diseño de los sistemas de vigilancia debería mantenerse confidencial ya que la divulgación puede facilitar las interrupciones no detectadas. Los sistemas de monitoreo deberían protegerse del acceso no autorizado para evitar que personas no autorizadas o sistemas que se deshabiliten de forma remota accedan a la información de vigilancia, como las fuentes de video. El panel de control del sistema de alarma debería colocarse en una zona de alarma y, para alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que establece la alarma. El panel de control y los detectores deberían tener mecanismos a prueba de manipulaciones. El sistema se debería probar regularmente para asegurarse de que funciona correctamente, especialmente si sus componentes funcionan con baterías. Cualquier mecanismo de monitoreo y grabación debería utilizarse tomando en consideración las leyes y normativas locales, incluida la protección de datos y la legislación de protección de IIP, especialmente en lo que respecta al monitoreo del personal y los períodos de retención de video grabado.					
OTRA INFORMACIÓN	No hay más información.					

7.5. PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y MEDIOAMBIENTALES

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección #Defensa	11.1.4
CONTROL	Debería diseñarse y aplicarse la protección contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.					
PROPÓSITO	Prevenir o reducir las consecuencias de los eventos originados por amenazas físicas y ambientales.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ORIENTACIÓN	Las evaluaciones de riesgos para identificar las consecuencias potenciales de las amenazas físicas y ambientales deberían realizarse antes de iniciar operaciones críticas en un sitio físico y a intervalos regulares. Se deberían aplicar las salvaguardias necesarias y se deberían supervisar los cambios en las amenazas. Se debería obtener asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y ambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos. La ubicación y la construcción de las instalaciones físicas deberían tener en cuenta: a) la topografía local, como elevación apropiada, cuerpos de agua y líneas de falla tectónica; b) las amenazas urbanas, como lugares con un alto perfil para atraer disturbios políticos, actividades delictivas o ataques terroristas. Sobre la base de los resultados de la evaluación de riesgos, deberían identificarse las amenazas físicas y ambientales pertinentes y considerarse los controles apropiados en los siguientes contextos como ejemplos: a) fuego: 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 en los medios de almacenamiento y en los sistemas de procesamiento de información relacionados. La extinción de incendios debería realizarse al utilizar la sustancia más apropiada con respecto al entorno circundante (por ejemplo, gas en espacios confinados); b) inundaciones: instalación de sistemas capaces de detectar inundaciones en una etapa temprana bajo los pisos de áreas que contienen medios de almacenamiento o sistemas de procesamiento de información. Las bombas de agua o los medios equivalentes deberían estar disponibles fácilmente en caso de que ocurra una inundación; c) sobretensiones eléctricas: adoptar sistemas capaces de proteger tanto los sistemas de información de servidor como de cliente contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de tales eventos; d) explosivos y armas: realización de inspecciones aleatorias por la presencia de explosivos o armas en personal, vehículos o mercancías que entran en instalaciones de procesamiento de información sensible.
OTRA INFORMACIÓN	Las cajas fuertes u otras formas de instalaciones seguras de almacenamiento pueden proteger la información almacenada en ellas contra desastres tales como incendios, terremotos, inundaciones o explosiones. Las organizaciones pueden considerar los conceptos de prevención del delito a través del diseño ambiental al diseñar los controles para asegurar su medio ambiente y reducir las amenazas urbanas. Por ejemplo, en lugar de utilizar balizas, las estatuas o los elementos de agua pueden servir tanto de característica como de barrera física.

7.6. TRABAJO EN ÁREAS SEGURAS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física**	**#Protección**	**11.1.5**
CONTROL	Deberían diseñarse y aplicarse medidas de seguridad para trabajar en zonas seguras.					
PROPÓSITO	Proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.					
ORIENTACIÓN	Las medidas de seguridad para trabajar en zonas seguras deberían aplicarse a todo el personal y abarcar todas las actividades que se realicen en la zona segura. Se deberían tomar en consideración las siguientes directrices: a) informar al personal de la existencia de, o actividades dentro de, un área segura; b) evitar el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades malintencionadas; c) bloquear físicamente e inspeccionar periódicamente las áreas seguras vacías; d) no permitir el uso de equipos de grabación, de video, audio o de fotografía, como cámaras en dispositivos finales de usuario, a menos que estén autorizados; e) controlar adecuadamente el transporte y el uso de los dispositivos de punto final del usuario en zonas seguras; f) publicar procedimientos de emergencia de forma fácilmente visible o accesible.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

OTRA INFORMACIÓN	No hay más información.

7.7. ESCRITORIO Y PANTALLA LIMPIOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad**	**#Proteger**	**#Seguridad_física**	**#Protección**	**11.2.9**
CONTROL	Se deberían definir y aplicar de forma adecuada reglas para papeles y medios de almacenamiento extraíbles en los escritorios, así como reglas de pantalla limpia para las instalaciones de procesamiento de información.					
PROPÓSITO	Reducir los riesgos de acceso no autorizado, pérdida y daños a la información en escritorios, pantallas y otros lugares accesibles durante y fuera del horario de trabajo normal.					
ORIENTACIÓN	La organización debería establecer y comunicar a todas las partes interesadas una política específica sobre el tema del escritorio ya la pantalla limpios. Se debería considerar: a) proteger la información organizacional confidencial o crítica (por ejemplo, en papel o en medios de almacenamiento electrónicos) (idealmente en una caja fuerte, armario u otro tipo de mobiliario de seguridad) cuando no sea necesario, especialmente cuando la oficina está desocupada; b) proteger los dispositivos finales de usuario mediante bloqueos de llave u otros medios de seguridad cuando no se utilizan o no están desatendidos; c) dejar los dispositivos de punto final de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando no están atendidos. Todos los equipos y sistemas deberían configurarse con una función de tiempo de espera o cierre de sesión automático; d) hacer que el originador recopile inmediatamente las salidas de impresoras o dispositivos multifunción. El uso de impresoras con una función de autenticación, por lo que los creadores son los únicos que pueden obtener sus impresiones y solo cuando se encuentran junto a la impresora; e) almacenar de forma segura documentos y medios de almacenamiento extraíbles que contengan información confidencial y, cuando ya no sea necesario, desecharlos mediante mecanismos de eliminación seguros; f) establecer y comunicar reglas y directrices 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 las presentaciones, el uso compartido de pantalla o en un área pública); g) borrar la información sensible o crítica de pizarras blancas y otros tipos de pantalla cuando ya no sea necesario. La organización debería disponer de procedimientos al desocupar las instalaciones, incluida la realización de un barrido final antes de salir para garantizar que los activos de la organización no se queden olvidados y desprotegidos (por ejemplo, documentos caídos detrás de cajones o muebles).					
OTRA INFORMACIÓN	No hay más información.					

7.8. UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física #Gestión_de_activos**	**#Protección**	**11.2.1**
CONTROL	Los equipos deberían ubicarse de forma segura y protegidos.					
PROPÓSITO	Reducir los riesgos derivados de amenazas físicas y ambientales, así como del acceso y los daños no autorizados.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ORIENTACIÓN	Se deberían tomar en consideración las siguientes directrices para proteger los equipos: a) ubicar los equipos de manera de minimizar el acceso innecesario a las zonas de trabajo y evitar el acceso no autorizado; b) ubicar cuidadosamente las instalaciones de procesamiento de información que manipulan datos sensibles para reducir el riesgo de que personas no autorizadas vean la información durante su uso; c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales (por ejemplo, robo, incendio, explosivos, humo, agua (o falla del suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencias de comunicaciones, radiación electromagnética y vandalismo); d) establecer directrices para comer, beber y fumar en proximidad a las instalaciones de procesamiento de información; e) controlar las condiciones ambientales, como la temperatura y la humedad, para condiciones que puedan afectar negativamente al funcionamiento de las instalaciones de procesamiento de información; f) aplicar protección pararrayos a todos los edificios e instalar filtros de protección contra rayos en todas las líneas de alimentación y comunicaciones entrantes; g) considerar el uso de métodos de protección especiales, como membranas de teclado, para equipos en entornos industriales; h) proteger los equipos que procesan información confidencial para minimizar el riesgo de pérdida de información debido a emanaciones electromagnéticas; i) separar físicamente las instalaciones de procesamiento de información gestionadas por la organización de las no gestionadas por la organización.
OTRA INFORMACIÓN	No hay más información.

7.9. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física #Gestión_de_activos**	**#Protección**	**11.2.6**
CONTROL	Los activos fuera de las instalaciones deberían estar protegidos.					
PROPÓSITO	Para evitar pérdidas, daños, robos o riesgos de dispositivos externos e interrupciones en las operaciones de la empresa.					
ORIENTACIÓN	Cualquier dispositivo utilizado fuera de las instalaciones de la empresa que almacene o procese información (por ejemplo, dispositivos móviles), incluidos los dispositivos propiedad de la empresa y los dispositivos de propiedad privada y utilizados en nombre de la organización (use su propio dispositivo (BYOD)) necesita protección. La administración debería autorizar el uso de estos dispositivos. Se deberían tener en cuenta las siguientes directrices para la protección de los dispositivos que almacenan o procesan información fuera de las instalaciones de la organización: a) no dejar el equipo y los medios de almacenamiento sin supervisión en lugares públicos y no protegidos; b) observar las instrucciones del fabricante para proteger los equipos en todo momento (por ejemplo, protección contra la exposición a campos electromagnéticos fuertes, agua, calor, humedad, polvo); c) mantener un registro que defina la cadena de custodia del equipo, incluidos al menos los nombres y organizaciones de los responsables del equipo, cuando el equipo fuera de las instalaciones se transfiere entre diferentes personas o partes interesadas. La información que no necesita transferirse con el activo debería eliminarse de forma segura antes de la transferencia; d) requerir autorización para retirar el equipo y los medios de comunicación de las instalaciones de la organización, cuando sea necesario y práctico, y que mantener un registro de dichas retiradas a fin de mantener un registro de auditoría (ver 5.14); e) proteger contra la visualización de información en los dispositivos (por ejemplo, móvil o portátil) en transporte público y los riesgos asociados con la navegación en el hombro; f) implementar el seguimiento de ubicación y capacidad para el borrado remoto de dispositivos.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	La instalación permanente de equipos fuera de las instalaciones de la organización (como antenas y cajeros automáticos (ATM)) puede estar sujeta a un mayor riesgo de daños, robo o espionaje. Estos riesgos pueden variar considerablemente de un lugar a otro y deberían tenerse en cuenta al determinar las medidas más adecuadas. Al situar este equipo fuera de las instalaciones de la organización, deberían tenerse en cuenta las siguientes directrices: a) supervisión de la seguridad física (ver 7.4); b) protección contra las amenazas físicas y medioambientales (ver 7.5); c) controles de acceso físico y de prueba de manipulación; d) control de acceso lógico.
OTRA INFORMACIÓN	Para más información sobre otros aspectos de la protección de equipos de almacenamiento y procesamiento de información y dispositivos finales de usuario ver 8.1 y 6.7.

7.10. MEDIOS DE ALMACENAMIENTO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física #Gestión_de_activos**	**#Protección**	**8.3.1 8.3.2 8.3.3 11.2.5**
CONTROL	Los medios de almacenamiento deberían gestionarse a través de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.					
PROPÓSITO	Garantizar únicamente la divulgación, modificación, eliminación o destrucción autorizada de la información en los medios de almacenamiento.					
ORIENTACIÓN	**<u>Medios de almacenamiento extraíbles</u>** Se deberían tener en cuenta las siguientes directrices para la gestión de medios de almacenamiento extraíbles: a) establecer una política específica de un tema sobre la administración de medios de almacenamiento extraíbles y comunicar dicha política a cualquier persona que utilice o gestione medios de almacenamiento extraíbles; b) cuando resulte necesario y práctico, exigir la autorización para el retiro de los soportes de almacenamiento de la organización y mantener un registro de dichos retiros con el fin de conservar un registro de auditoría; c) almacenar todos los medios de almacenamiento en un entorno seguro y seguro según su clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, humedad, campo electrónico o envejecimiento), de conformidad con las especificaciones de los fabricantes; d) si la confidencialidad o integridad de la información son consideraciones importantes, utilizar técnicas cifradas para proteger la información en medios de almacenamiento extraíbles; e) para mitigar el riesgo de degradación de los medios de almacenamiento mientras aún se necesita información almacenada, transferir la información a medios de almacenamiento nuevos antes de que sea ilegible; f) almacenar varias copias de información valiosa en medios de almacenamiento independientes para reducir aún más el riesgo de daños o pérdidas de información fortuita; g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información; h) solo habilitar puertos de medios de almacenamiento extraíbles (por ejemplo, ranuras para tarjetas Secure Digital (SD) y puertos USB (bus universal en serie)) si existe un motivo de organización para su uso; i) cuando sea necesario utilizar medios de almacenamiento extraíbles, supervisando 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 a través del servicio de mensajería. En este control, el material incluye documentos impresos. Al transferir medios de almacenamiento físicos, aplique medidas de seguridad en 5.14.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Reutilización o eliminación segura Deberían establecerse procedimientos para la reutilización o eliminación segura de los medios de almacenamiento a fin de reducir al mínimo el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación segura de los medios de almacenamiento que contienen información confidencial deberían ser proporcionales a la sensibilidad de dicha información. Se deberían tomar en consideración los siguientes factores: a) si es necesario reutilizar los medios de almacenamiento que contienen información confidencial dentro de la organización, elimine los datos de forma segura o formatee los medios de almacenamiento antes de volver a utilizarlos (ver 8.10); b) desechar los medios de almacenamiento que contienen información confidencial de forma segura cuando ya no sea necesario (por ejemplo, destruir, triturar o eliminar el contenido de forma segura); c) disponer de procedimientos para identificar los elementos que pueden requerir una eliminación segura; d) muchas organizaciones ofrecen servicios de recogida y eliminación de medios de almacenamiento. Se debería tener cuidado al seleccionar un proveedor externo adecuado con controles y experiencia adecuados; e) registrar la eliminación de elementos sensibles para mantener un registro de auditoría; f) al acumular medios de almacenamiento para su eliminación, tomando en consideración el efecto de agregación, que puede hacer que una gran cantidad de información no confidencial se vuelva sensible. Se debería realizar una evaluación de riesgos en los dispositivos dañados que contengan datos sensibles para determinar si los elementos deberían destruirse físicamente en lugar de enviarse para su reparación o descartarse (ver 7.14).
OTRA INFORMACIÓN	Cuando la información confidencial de los medios de almacenamiento no está cifrada, debería considerarse la protección física adicional de los medios de almacenamiento.

7.11. SERVICIOS PÚBLICOS DE RESPALDO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Detectivo	**#Integridad #Disponibilidad**	**#Proteger #Detectar**	**#Seguridad_física**	**#Protección**	**11.2.2**
CONTROL	Las instalaciones de procesamiento de la información deberían estar protegidas contra los cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de respaldo.					
PROPÓSITO	Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la organización debido al fracaso y la interrupción de los servicios públicos de respaldo.					
ORIENTACIÓN	Las organizaciones dependen de los servicios públicos (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, aguas residuales, ventilación y aire acondicionado) para apoyar sus instalaciones de procesamiento de información. Por lo tanto, deberían: a) asegurarse de que el equipo que soporta los servicios está configurado operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente; b) garantizar que los servicios públicos sean evaluados periódicamente en cuanto a su capacidad para satisfacer el crecimiento de la empresa y las interacciones con otros servicios de respaldo; c) garantizar que los equipos de soporte de los servicios públicos se inspeccionen y prueben regularmente para garantizar su correcto funcionamiento; d) levantar alarmas para detectar fallas de funcionamiento de los servicios públicos, si es necesario; e) asegurarse de que los servicios públicos tienen varias fuentes con enrutamiento físico diverso, si es necesario; f) garantizar que los equipos que soportan los servicios públicos estén en una red separada de las instalaciones de procesamiento de la información, si están conectadas a una red; g) garantizar que los equipos que soportan los servicios públicos se conecten a Internet solo cuando sea necesario y de forma segura. Se deberían proporcionar iluminación de emergencia y comunicaciones. Los interruptores y válvulas de emergencia para cortar la alimentación, el agua, el gas u otros servicios públicos deberían estar ubicados cerca de las salidas de emergencia o de las salas de equipos. Los datos de					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	contacto de emergencia deberían registrarse y ponerse a disposición del personal en caso de interrupción del servicio.
OTRA INFORMACIÓN	Se puede obtener redundancia adicional para la conectividad de red mediante varias rutas de más de un proveedor de servicios públicos.

7.12. SEGURIDAD DEL CABLEADO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Disponibilidad**	**#Proteger**	**#Seguridad_física**	**#Protección**	**11.2.3**
CONTROL	Los cables que transportan energía, datos o servicios de información de respaldo deberían estar protegidos contra la interceptación, las interferencias o los daños.					
PROPÓSITO	Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la organización debido al cableado de alimentación y comunicaciones.					
ORIENTACIÓN	Se deberían tener en cuenta las siguientes directrices para la seguridad del cableado: a) líneas de energía y telecomunicaciones en instalaciones de procesamiento de información bajo tierra siempre que sea posible o sometidas a una protección alternativa adecuada, como el protector de cables de suelo y el polo de a tierra; si los cables están bajo tierra, deberían estar protegidos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia); b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias; c) para sistemas sensibles o críticos otros controles a considerar incluyen: 1) instalación de conductos blindados y salas o cajas bloqueadas y alarmas en los puntos de inspección y terminación; 2) uso de blindaje electromagnético para proteger los cables; 3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados que se conectan a los cables; 4) acceso controlado a paneles de conexiones y salas de cables (por ejemplo, con llaves mecánicas o PINES); 5) uso de cables de fibra óptica; d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable. Se debería solicitar asesoramiento especializado sobre cómo gestionar los riesgos derivados de incidentes o fallas de funcionamiento del cableado.					
OTRA INFORMACIÓN	A veces, el cableado de energía y telecomunicaciones es un recurso compartido para más de una organización que ocupa instalaciones ubicadas en una misma ubicación.					

7.13. MANTENIMIENTO DE EQUIPOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_física #Gestión_de_activos**	**#Protección #Resiliencia**	**11.2.4**
CONTROL	Los equipos deberían mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.					
PROPÓSITO	Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la organización debido al cableado de alimentación y comunicaciones.					
ORIENTACIÓN	Se deberían tener en cuenta las siguientes directrices para el mantenimiento del equipo: a) mantener el equipo de acuerdo con la frecuencia de servicio y las especificaciones recomendadas por el proveedor; b) ejecutar y hacer seguimiento a un programa de mantenimiento por parte de la organización; c) realizar las reparaciones y el mantenimiento de los equipos solo por el personal de mantenimiento autorizado; d) mantener registros de todas las averías sospechosas o reales, así como de todo					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	mantenimiento preventivo y correctivo; e) implementar controles adecuados cuando el equipo esté programado para el mantenimiento, tomando en consideración si este mantenimiento lo realiza el personal del emplazamiento o externo a la organización; someter al personal de mantenimiento a un acuerdo de confidencialidad adecuado; f) supervisar al personal de mantenimiento durante el mantenimiento in situ; g) autorizar y controlar el acceso para el mantenimiento remoto; h) aplicar medidas de seguridad para los activos fuera de las instalaciones (ver 7.9) si el equipo que contiene información se desocupa de las instalaciones para su mantenimiento; i) cumplir todos los requisitos de mantenimiento impuestos por el seguro; j) antes de volver a poner el equipo en funcionamiento después del mantenimiento, se debería inspeccionar para asegurarse de que el equipo no se ha manipulado y funciona correctamente; k) aplicar medidas para la eliminación o reutilización seguras del equipo (ver 7.14) si se determina que el equipo se va a desechar.
OTRA INFORMACIÓN	El equipo incluye componentes técnicos de instalaciones de procesamiento de información, sistemas de alimentación ininterrumpida (UPS) y baterías, generadores de energía, alternadores y convertidores de potencia, sistemas y alarmas de detección de intrusiones físicas, detectores de humo, extintores de incendios, aire acondicionado y ascensores.

7.14. ELIMINACIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad**	**#Proteger**	**#Seguridad_física #Gestión_de_activos**	**#Protección**	**11.2.7**
CONTROL	Los elementos de los equipos que contienen medios de almacenamiento deberían verificarse para garantizar que los datos confidenciales y el software con licencia se han eliminado o sobrescrito de forma segura antes de desecharlos o reutilizarlos.					
PROPÓSITO	Evitar fugas de información del equipo que se va a desechar o reutilizar.					
ORIENTACIÓN	El equipo se debería verificar para asegurarse de que los medios de almacenamiento están contenidos o no antes de su eliminación o reutilización. Los medios de almacenamiento que contienen información confidencial o protegida por derechos de autor deberían destruirse físicamente o la información debería destruirse, eliminarse o sobrescribirse al utilizar técnicas para que la información original no pueda recuperarse en lugar de utilizar la función de eliminación convencional. Ver 7.10 para obtener guía detallada sobre la eliminación segura de los medios de almacenamiento y el 8.10 para obtener guía sobre la eliminación de información. Las etiquetas y las marcas que identifiquen a la organización o indiquen la clasificación, propietario, sistema o red, deberían eliminarse antes de su disposición final, esto incluye la reventa o donación a una organización benéfica. 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 de las instalaciones. Esto depende de factores como: a) su contrato de arrendamiento para devolver la instalación a su condición original; b) minimizar el riesgo de dejar sistemas con información confidencial para el siguiente arrendatario (por ejemplo, listas de acceso de usuarios, archivos de video o de imágenes); c) la capacidad de reutilizar los controles en la siguiente instalación.					
OTRA INFORMACIÓN	Los equipos dañados que contienen medios de almacenamiento pueden requerir una evaluación de riesgos para determinar si los elementos deberían destruirse físicamente en lugar de enviarse para su reparación o descartarse. La información puede verse comprometida por la eliminación descuidada o la reutilización del equipo. Además de la eliminación segura del disco, el cifrado de disco completo reduce el riesgo de revelación de información confidencial cuando se desecha o se vuelve a implementar el equipo, siempre que: a) el proceso de cifrado sea suficientemente sólido y cubra todo el disco (incluido el espacio libre, los archivos de intercambio);					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	b) las claves cifradas sean lo suficientemente largas como para resistir los ataques de fuerza bruta; c) las claves cifradas se mantienen en sí mismas como confidenciales (por ejemplo, nunca se almacenan en el mismo disco). Para más consejos sobre cifrado, ver 8.24. Las técnicas para sobrescribir de forma segura los medios de almacenamiento difieren según la tecnología de los medios de almacenamiento y el nivel de clasificación de la información contenida en los medios de almacenamiento. Las herramientas de sobreescritura deberían revisarse para asegurarse de que sean aplicables a la tecnología de los medios de almacenamiento. Información detallada sobre los métodos de desinfección de los medios de almacenamiento en la norma ISO/IEC 27040.

8. CONTROLES TECNOLÓGICOS

8.1. DISPOSITIVOS DEL PUNTO FINAL DEL USUARIO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_activos #Protección_de_la_información**	**#Protección**	**6.2.1 11.2.8**
CONTROL	La información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario debería estar protegida.					
PROPÓSITO	Proteger la información contra los riesgos introducidos mediante el uso de dispositivos de punto final del usuario (user endpoints).					
ORIENTACIÓN	**General** La organización debería establecer una política específica sobre la configuración y el manejo seguros de los dispositivos de punto final del usuario. La política específica del tema debería comunicarse a todo el personal pertinente y considerar lo siguiente: a) tipo de información y el nivel de clasificación que los dispositivos de punto final del usuario pueden gestionar, procesar, almacenar o admitir; b) registro de dispositivos de punto final del usuario; c) requisitos de protección física; d) restricción de la instalación de software (por ejemplo, controlado de forma remota por los administradores del sistema); e) requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para 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, que requiera el uso de cortafuegos personal); g) controles de acceso; h) cifrado de dispositivos de almacenamiento; i) protección contra malware; j) desactivación, eliminación o bloqueo remotos; k) copias de seguridad; l) uso de servicios web y aplicaciones web; m) análisis del comportamiento del usuario final (ver 8.16); n) el uso de dispositivos extraíbles, incluidos dispositivos de memoria extraíbles y la posibilidad de desactivar puertos físicos (por ejemplo, Puertos USB); o) el uso de capacidades de partición, si es compatible con el dispositivo final del usuario, que puede separar de forma segura la información de la empresa y otros activos asociados (por ejemplo, software) de otra información y otros activos asociados del dispositivo. Se debería considerar si cierta información es tan sensible que solo se puede acceder a ella a través de dispositivos de punto final de usuario, pero no se puede almacenar en dichos dispositivos. En tales casos, se pueden requerir protecciones técnicas adicionales en el dispositivo. Por ejemplo, asegurarse de que la descarga de archivos para trabajar sin conexión está desactivada y de que el almacenamiento local, como la tarjeta SD, está desactivado.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	En la medida de lo posible, las recomendaciones sobre este control se deberían aplicar mediante la administración de la configuración (ver 8.9) o mediante herramientas automatizadas. **Responsabilidades del usuario** Todos los usuarios deberían ser conscientes de los requisitos y procedimientos de seguridad para proteger los dispositivos de punto final de los usuarios, así como de sus responsabilidades para implementar dichas medidas de seguridad. Se debería aconsejar a los usuarios: a) cerrar la sesión activa y terminar servicios cuando ya no sean necesarios; b) proteger los dispositivos de punto final del usuario de un uso no autorizado con un control físico (por ejemplo, bloqueo con llave o bloqueos especiales) y un control lógico (por ejemplo, acceso con contraseña) cuando no se estén al utilizar; no dejar desatendidos los dispositivos que lleven 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 la lectura de información confidencial si las personas pueden leer desde la parte posterior, utilizar filtros de pantalla de privacidad); d) proteger físicamente los dispositivos finales de usuario contra robos (por ejemplo, en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión). Para los casos de robo o pérdida de dispositivos final de usuario se debería establecer un procedimiento específico que tenga en cuenta los requisitos legales, legales, reglamentarios, contractuales (incluidos seguros) y otros requisitos de seguridad de la organización. **Uso de dispositivos personales** Cuando la empresa permite el uso de dispositivos personales (BYOD), además de las directrices proporcionadas en este control, se debería tener en cuenta lo siguiente: a) separar el uso personal y organizacional de los dispositivos, incluido el uso de software para admitir dicha separación y proteger los datos organizacionales en un dispositivo privado; b) proporcionar acceso a la información empresarial solo después de que los usuarios hayan reconocido sus obligaciones (protección física, actualización de software, etc.), renunciar a la propiedad de los datos organizacionales, permitir el borrado remoto de los datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no esté autorizado a utilizar el servicio. En tales casos, debería considerarse la legislación de protección de la IIP; c) establecer políticas y procedimientos específicos para prevenir controversias relativas a los derechos de propiedad intelectual sobre equipos de propiedad privada; d) impedir el acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), si lo requiere la legislación; e) establecer o respetar acuerdos de licencia de software para que la organización pueda hacerse responsables de la licencia del software cliente en dispositivos finales de usuario propiedad privada del personal o de usuarios externos. **Conexiones inalámbricas** La organización debería establecer procedimientos para: a) la configuración de las conexiones inalámbricas en los dispositivos (por ejemplo, desactivar protocolos vulnerables); b) utilizar conexiones inalámbricas o con cable con el ancho de banda adecuado de acuerdo con las políticas específicas de cada tema (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de software).
OTRA INFORMACIÓN	Los controles para proteger la información de los dispositivos finales de usuario dependen de si el dispositivo final de usuario se utiliza solo dentro de las instalaciones seguras y las conexiones de red de la empresa o si está expuesto a mayores amenazas físicas y relacionadas con la red fuera de la organización. Las conexiones inalámbricas para los dispositivos de punto final de usuario son similares a otros tipos de conexiones de red, pero tienen diferencias importantes que deberían tenerse en cuenta al identificar los controles. En particular, la copia de SI 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 el momento en que se programan las copias de seguridad. Para algunos puertos USB, como USB-C, no es posible desactivar el puerto USB porque se utiliza para otros fines (por ejemplo, suministro de energía y salida de pantalla).

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

8.2. DERECHOS DE ACCESO PRIVILEGIADOS

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_la_identidad_y_del_acceso	#Protección	9.2.3
CONTROL	La asignación y el uso de los derechos de acceso privilegiados deberían ser restringidos y gestionados.					
PROPÓSITO	Garantizar que solo los usuarios autorizados, los componentes de software y los servicios se proporcionan con derechos de acceso privilegiados.					
ORIENTACIÓN	La asignación de derechos de acceso privilegiado debería controlarse mediante un proceso de autorización de acuerdo con una política de control de acceso específica (ver 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 privilegiados a los usuarios según sea necesario y evento por evento, de acuerdo con la política de control de acceso específica de cada tema (ver 5.15) (es decir, solo a personas con la competencia necesaria para realizar actividades que requieran acceso privilegiados y basadas en el requisito mínimo de sus funciones funcionales); c) mantener un proceso de autorización (es decir, determinar quién puede aprobar los derechos de acceso privilegiados o no conceder derechos de acceso privilegiados hasta que se complete el proceso de autorización) y un registro de todos los privilegios asignados; d) definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado; e) tomar medidas para garantizar que los usuarios conozcan sus derechos de acceso privilegiado y cuando se encuentren 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 un equipo específico; f) volver a realizar la autenticación o la autenticación antes de trabajar con derechos de acceso privilegiados si es necesario, ya que los requisitos de autenticación para los derechos de acceso privilegiados pueden ser superiores a los requisitos para los derechos de acceso normales; g) revisar, regularmente y después de cualquier cambio en la organización, a los usuarios que trabajan con derechos de acceso privilegiados, para verificar si sus deberes, funciones, responsabilidades y competencias aún los califican para trabajar con derechos de acceso privilegiados (ver 5.18); h) establecer reglas específicas para evitar el uso de ID de usuario de administración genéricos (como “admin”), dependiendo de las capacidades de configuración de los sistemas. Administrar y proteger la información de autenticación de dichas identidades (ver 5.17); i) conceder acceso temporal con privilegios solo durante el período de tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de conceder derechos de acceso privilegiados de forma permanente. A menudo, esto se denomina procedimiento de ventanilla y a menudo está automatizado mediante tecnologías de gestión de acceso de privilegios; j) registrar todo acceso privilegiado a los sistemas con fines de auditoría; k) no compartir o vincular identidades con derechos de acceso privilegiados a varias personas, asignando a cada persona una identidad independiente que permita asignar derechos de acceso privilegiados específicos. Las identidades se pueden agrupar (por ejemplo, mediante la definición de un grupo de administradores) para simplificar la gestión de los derechos de acceso privilegiados; l) utilizar solamente identidades con derechos de acceso privilegiados para realizar tareas administrativas y no para tareas generales diarias (es decir, comprobar el correo electrónico, acceder a la web (los usuarios deberían tener una identidad de red normal					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	independiente para estas actividades)).
OTRA INFORMACIÓN	Los derechos de acceso privilegiados son derechos de acceso proporcionados a una identidad, una función o un proceso que permite realizar actividades que los usuarios o procesos típicos no pueden realizar. Las funciones de administrador del sistema normalmente requieren derechos de acceso privilegiados. El uso inapropiado de los privilegios del 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 un factor importante que contribuye a las fallas o incumplimientos de los sistemas. Más información relacionada con la gestión del acceso y la gestión segura del acceso a la información y a los recursos de tecnologías de la información y las comunicaciones en la norma ISO/IEC 29146.

8.3. RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_la_identidad_y_del_accesos**	**#Protección**	**9.4.1**
CONTROL	El acceso a la información y a otros activos asociados debería restringirse de conformidad con la política establecida sobre el control del acceso relativa a temas específicos.					
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 a otros activos asociados debería restringirse de conformidad con las políticas establecidas sobre temas específicos. Se debería tener en cuenta lo siguiente para admitir los requisitos de restricción de acceso: a) no permitir el acceso a información confidencial por identidades de usuario desconocidas o anónimas. El acceso público o anónimo solo debería concederse a ubicaciones de almacenamiento que no contengan información confidencial; b) proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios; c) controlar a qué datos puede acceder un usuario concreto; d) controlar qué identidades o grupos de identidades tienen acceso, como lectura, escritura, eliminación y ejecución; e) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones, datos de aplicaciones o sistemas confidenciales. Además, las técnicas y procesos de gestión de acceso dinámico para proteger la información confidencial que tiene un alto valor para la organización deberían considerarse cuando la organización: a) necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera; b) desea compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a ella; c) desea gestionar dinámicamente, en tiempo real, el uso y la distribución de dicha información; d) desea proteger dicha información contra cambios, copias y distribución no autorizados (incluida la impresión); e) quiere controlar el uso de la información; f) desea registrar cualquier cambio en dicha información que tenga lugar en caso de que se requiera una investigación futura. Las técnicas de gestión dinámica de acceso deberían proteger la información a lo largo de su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluidos: a) establecer reglas sobre la gestión del acceso dinámico basadas en casos de uso específicos considerando: 1) conceder permisos de acceso basados en la identidad, el dispositivo, la ubicación o la aplicación; 2) aprovechar el esquema de clasificación para determinar qué información necesita					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	protegerse con técnicas de gestión de acceso dinámico; b) establecer procesos operacionales, de supervisión y de presentación de informes y de infraestructura técnica de apoyo. Los sistemas de gestión de acceso dinámico deberían proteger la información mediante: a) solicitud de autenticación, credenciales adecuadas o un certificado para acceder a la información; b) restricción del acceso, por ejemplo, a un plazo de tiempo especificado (por ejemplo, después de una fecha determinada o hasta una fecha determinada); c) uso del cifrado para proteger la información; d) definición de los permisos de impresión para la información; e) registro de quién accede a la información y cómo se utiliza; f) aumento de alertas al detectar intentos de hacer un uso incorrecto de la información.
OTRA INFORMACIÓN	Las técnicas de gestión de acceso dinámico y otras tecnologías de protección dinámica pueden admitir 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 ser adaptado a lo largo del ciclo de vida de la información. Las técnicas de gestión dinámica de acceso no sustituyen a la gestión clásica de acceso (por ejemplo, el uso de listas de control de acceso (ACL)), sino que pueden añadir más factores para la condicionalidad, la evaluación en tiempo real, la reducción de datos justo a tiempo y otras mejoras que pueden ser útiles para la información más sensible. Ofrece una forma de controlar el acceso fuera del entorno de la organización. Las técnicas de gestión de acceso dinámico pueden admitir la respuesta a incidentes ya que los permisos se pueden modificar o revocar en cualquier momento. 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	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_identidades_y_accesos #Seguridad_de_las_aplicaciones #Configuración_segura**	**#Protección**	**9.4.5**
CONTROL	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se deberían administrar adecuadamente.					
PROPÓSITO	Para evitar la introducción de funciones no autorizadas, evite cambios no intencionados o malintencionados y mantenga la confidencialidad de la propiedad intelectual valiosa.					
ORIENTACIÓN	El acceso al código fuente y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y a las herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas de prueba y entornos) deberían controlarse rigurosamente. Para el código fuente, esto se puede lograr al controlar el almacenamiento centralizado de dicho código, preferiblemente en el sistema de gestión del código fuente. El acceso de lectura y escritura al código fuente puede variar en función de la función del personal. Por ejemplo, el acceso de lectura al código fuente se puede proporcionar ampliamente dentro de la organización, pero el acceso de escritura al código fuente solo está disponible para el personal con privilegios o los propietarios designados. Cuando varios desarrolladores de una organización utilizan componentes de código, se debería implementar el acceso de lectura a un repositorio de código centralizado. Además, si se utiliza código de código abierto o componentes de código de terceros dentro de una organización, se puede proporcionar acceso de lectura a dichos repositorios de código externo. Sin embargo, el acceso de escritura debería seguir estando restringido. Se deberían considerar las siguientes directrices para controlar el acceso a las bibliotecas de origen de programas a fin de reducir el potencial de corrupción de los programas informáticos:					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	a) administrar el acceso al código fuente del programa y a las bibliotecas de origen del programa según los procedimientos establecidos; b) conceder acceso de lectura y escritura al código fuente en función de las necesidades empresariales y gestionar para abordar los riesgos de alteración o uso indebido y de acuerdo con los procedimientos establecidos; c) actualizar el código fuente y los elementos asociados y conceder acceso al código fuente de acuerdo con los procedimientos de control de cambios (ver 8.32) y realizarlo solo después de recibir la autorización adecuada; 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 en el código fuente; e) mantener listas de programas en un entorno seguro, donde el acceso de lectura y escritura debería gestionarse y asignarse de forma adecuada; f) mantener un registro de auditoría de todos los accesos y de todos los cambios realizados en el código fuente. Si se pretende publicar el código fuente del programa, deberían considerarse controles adicionales para garantizar su integridad (por ejemplo, la firma digital).
OTRA INFORMACIÓN	Si el acceso al código fuente no se controla correctamente, el código fuente se puede modificar o algunos datos del entorno de desarrollo (por ejemplo, copias de datos de producción, detalles de configuración) pueden ser recuperados por personas no autorizadas.

8.5. AUTENTICACIÓN SEGURA

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Gestión_de_identidades_y_accesos**	**#Protección**	**9.4.2**
CONTROL	Las tecnologías y los procedimientos de autenticación segura deberían implementarse en función de las restricciones de acceso a la información y de la política de control de acceso específica del tema.					
PROPÓSITO	Garantizar que un usuario o una entidad se autentique de forma segura cuando se conceda acceso a sistemas, aplicaciones y servicios.					
ORIENTACIÓN	Debería elegirse una técnica de autenticación adecuada para fundamentar la identidad declarada de un usuario, software, mensajes y otras entidades. La solidez de la autenticación debería ser adecuada para la clasificación de la información a la que se va a acceder. Cuando se requiere autenticación y verificación de identidad sólidas, se utilizan métodos de autenticación se debería utilizar una alternativa a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos. La información de autenticación debería ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información críticos (también conocidos como autenticación de varios factores). El uso de una combinación de varios factores de autenticación, como lo que sabe, lo que tiene y lo que es, reduce las posibilidades de accesos no autorizados. La autenticación de varios factores se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, basados en reglas y patrones predefinidos, como el acceso desde una ubicación inusual, desde un dispositivo inusual o en un momento inusual. La información de autenticación biométrica debería invalidarse si alguna vez se ve comprometida. La autenticación biométrica puede no estar disponible dependiendo de las condiciones de uso (por ejemplo, humedad o envejecimiento). Para prepararse para estos problemas, la autenticación biométrica debería ir acompañada de al menos una técnica de autenticación alternativa. El procedimiento para iniciar sesión en un sistema o aplicación debería diseñarse para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión deberían implementarse tomando en consideración lo siguiente: a) no mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado correctamente para evitar que un usuario no autorizado reciba asistencia innecesaria; b) mostrar un aviso general advirtiendo de que el sistema, la aplicación o el servicio solo deberían ser accesibles por usuarios autorizados;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayuden a un usuario no autorizado (por ejemplo, si se produce una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta); d) validar la información de inicio de sesión solo cuando se completen todos los datos de entrada; e) proteger contra intentos de inicio de sesión de forzada en nombres de usuario y contraseñas (por ejemplo, mediante una prueba de Turing pública y automática para distinguir a los computadores de los humanos (CAPTCHA), que requiere el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o que bloquea al usuario después de un número máximo de errores); f) registrar los intentos fallidos y correctos; g) provocar un evento de seguridad si se detecta un posible intento o incumplimiento satisfactorio de los controles de inicio de sesión (por ejemplo, enviar una alerta al usuario y a los administradores del sistema de la empresa cuando se ha alcanzado un número determinado de intentos de contraseña incorrectos); h) visualizar o enviar de la siguiente información en un canal separado al finalizar un inicio de sesión correcto: 1) fecha y hora del inicio de sesión anterior correcto; 2) detalles de cualquier intento de inicio de sesión incorrecto desde el último inicio de sesión correcto; i) no mostrar una contraseña en texto no cifrado al introducirla; en algunos casos, puede ser necesario desactivar esta función para facilitar el inicio de sesión del usuario (por ejemplo, por motivos de accesibilidad o para evitar bloquear a los usuarios debido a errores repetidos); j) no transmitir contraseñas en texto no cifrado a través de una red para evitar ser capturadas por un programa de rastreador de red; k) finalizar sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo, como áreas públicas o externas fuera de la gestión de seguridad de la organización o en dispositivos 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 oportunidad de acceso no autorizado.
OTRA INFORMACIÓN	Información adicional sobre la garantía de autenticación de entidades en la norma ISO/IEC 29115.

8.6. GESTIÓN DE LA CAPACIDAD

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Detectivo	**#Integridad #Disponibilidad**	**#Identificar #Proteger #Detectar**	**#Continuidad**	**#Gobierno_y_ecosistema #Protección**	**12.1.3**
CONTROL	La utilización de los recursos debería supervisarse y ajustarse de conformidad con las necesidades de capacidad actuales y previstas.					
PROPÓSITO	Garantizar la capacidad necesaria de los servicios de procesamiento de información, los recursos humanos, las oficinas y otros servicios.					
ORIENTACIÓN	Deberían determinarse las necesidades de capacidad para las instalaciones de procesamiento de información, los recursos humanos, las oficinas y otras instalaciones, tomando en consideración la importancia empresarial de los sistemas y procesos en cuestión. El ajuste y la supervisión del sistema deberían aplicarse para garantizar y, en caso necesario, mejorar la disponibilidad y la eficiencia de los sistemas. La organización debería realizar pruebas de esfuerzo de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema para satisfacer los requisitos de rendimiento máximo. Los controles de detección deberían ponerse en marcha para indicar problemas oportunamente. Las proyecciones de los requisitos de capacidad futuros deberían tener en cuenta los nuevos requisitos organizacionales y del sistema, así como las tendencias actuales y proyectadas de las capacidades de procesamiento de información de la organización. Se debería prestar especial atención a los recursos con plazos de entrega largos o costos					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	elevados. Por lo tanto, los administradores, los propietarios de servicios o productos deberían supervisar la utilización de los recursos clave del sistema. Los administradores deberían utilizar la información de capacidad para identificar y evitar posibles limitaciones de recursos y dependencia del personal clave que pueda representar una amenaza para la seguridad o los servicios del sistema y planificar las medidas apropiadas. Se puede lograr una capacidad suficiente aumentando la capacidad o reduciendo la demanda. Se deberían tomar en consideración las siguientes directrices para aumentar la capacidad: a) contratación de nuevo personal; b) obtención de nuevas instalaciones o espacio; c) adquisición de sistemas de procesamiento, memoria y almacenamiento más potentes; d) uso de computación en la nube (cloud computing), que tiene características inherentes que abordan directamente los problemas de capacidad. La computación en nube tiene elasticidad y escalabilidad que permiten una rápida expansión y reducción bajo demanda de los recursos disponibles para aplicaciones y servicios específicos. Para reducir la demanda de los recursos de la organización, se debería tener en cuenta lo siguiente: a) eliminación de datos obsoletos (espacio en disco); b) eliminación de registros impresos que hayan cumplido su período de retención (liberar espacio para estanterías); c) clausura de aplicaciones, sistemas, bases de datos o entornos; d) optimización de procesos por lotes y programaciones; e) optimización del código de aplicación o de las consultas a la base de datos; f) rechazo o restricción del ancho de banda para servicios que consumen recursos si no son críticos (por ejemplo, transmisión de video). Debería considerarse un plan de gestión de la capacidad documentado para los sistemas de misión crítica.
OTRA INFORMACIÓN	Más información sobre la elasticidad y escalabilidad de la computación en la nube en la norma ISO/IEC TS 23167.

8.7. PROTECCIÓN CONTRA MALWARE

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Detectivo #Correctivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger #Detectar**	**#Seguridad_deñ_sistema_y_de_la_red #Protección_de_la_información**	**#Protección #Defensa**	**12.2.1**
CONTROL	La protección contra el malware debería implementarse y respaldarse con el conocimiento adecuado del usuario.					
PROPÓSITO	Garantizar que la información y otros activos asociados estén protegidos contra malware.					
ORIENTACIÓN	La protección contra el malware debería basarse en software de detección y reparación de malware, conocimiento de la SI, acceso adecuado al sistema y controles de gestión de cambios. El uso de software de detección y reparación de malware por sí solo no suele ser adecuado. Se deberían tomar en consideración las siguientes directrices: a) implementar reglas y controles que impidan o detecten el uso de software no autorizado (por ejemplo, lista de aplicaciones permitidas (por ejemplo, utilizar una lista que proporcione aplicaciones permitidas)) (ver 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 malware (por ejemplo, mediante la gestión de vulnerabilidades técnicas (ver 8.8 y 8.19)); d) realizar una validación automatizada regular del software y del contenido de datos de los sistemas, especialmente para los sistemas que soportan procesos organizacionales críticos; investigar la presencia de archivos no aprobados o modificaciones no autorizadas; e) establecer medidas de protección contra los riesgos asociados a la obtención de					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	archivos y software ya sea desde o a través de redes externas o en cualquier otro medio; f) instalar y actualizar periódicamente el software de detección y reparación de malware para analizar computadores y medios de almacenamiento electrónicos. Realización de exploraciones regulares que incluyen: 1) analizar cualquier dato recibido a través de redes o a través de cualquier medio de almacenamiento electrónico en busca de malware antes de su uso; 2) analizar archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso. Realizar este análisis en diferentes lugares (por ejemplo, en servidores de correo electrónico computadores de escritorio) y al entrar en la red de la organización; 3) analizar páginas web en busca de malware cuando se accede a ellas; g) determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los resultados de la evaluación de riesgos y considerar: 1) defensa en profundidad principios en los que serían más eficaces. Por ejemplo, esto puede llevar a la detección de malware en una puerta de enlace de red (en varios protocolos de aplicación como correo electrónico, transferencia de archivos y web), así como en dispositivos y servidores de extremo de usuario; 2) las técnicas evasivas de los atacantes (por ejemplo, el uso de archivos cifrados) para ofrecer malware o el uso de protocolos de cifrado para transmitir malware; h) cuidar de la protección contra la introducción de malware durante el mantenimiento y los procedimientos de emergencia, que pueden eludir los controles normales contra el malware; i) implementar un proceso para autorizar temporalmente o permanentemente la desactivación de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra el malware provoca interrupciones en las operaciones normales; j) preparar planes de continuidad empresarial adecuados para la recuperación de ataques de malware, incluidos todos los datos y copias de seguridad de software necesarios (incluidas las copias de seguridad online y offline) y las medidas de recuperación (ver 8.13); k) aislar los entornos en los que pueden producirse consecuencias catastróficas; l) definir procedimientos y responsabilidades para tratar la protección contra el malware en los sistemas, incluida la formación sobre su uso, la elaboración de informes y la recuperación de ataques de malware; m) proporcionar conocimientos o formación (ver 6.3) a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados por malware (la información recopilada en n) y o) puede utilizarse para garantizar que la concienciación y la formación se mantienen al día); n) implementar procedimientos para recopilar periódicamente información sobre nuevos programas maliciosos, como la suscripción a listas de correo o la revisión de sitios web relevantes; o) verificar que la información relacionada con el malware, como los boletines de advertencia, proviene de fuentes calificadas y fiables (por ejemplo, sitios de internet fiables o proveedores de software de detección de malware) y es precisa e informativa.
OTRA INFORMACIÓN	No siempre es posible instalar software que proteja contra el malware en algunos sistemas (por ejemplo, algunos sistemas de control industrial). Algunas formas de malware infectan los sistemas operativos del computador y el firmware del computador, de forma que los controles de malware comunes no pueden limpiar el sistema y es necesario volver a crear una imagen completa del software del sistema operativo y, a veces, el firmware del computador para volver a un estado seguro.

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

8.8. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión_de_amenazas_y_vulnerabilidades	#Gobierno_y_ecosistema #Protección #Defesa	12.6.1 18.2.3

CONTROL	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debería evaluar la exposición de la organización a esas vulnerabilidades y se deberían adoptar las medidas apropiadas.
PROPÓSITO	Evitar la explotación de vulnerabilidades técnicas.
ORIENTACIÓN	**Identificación de vulnerabilidades técnicas** La organización debería tener un inventario preciso de los activos (ver 5.9 al 5.14) como requisito previo para una gestión eficaz de la vulnerabilidad técnica; el inventario debería incluir el proveedor del software, el nombre del software, los números de versión, el estado actual de la implementación (por ejemplo, qué software está instalado en qué sistemas) y la persona o personas dentro de la organización responsable del software. Para identificar vulnerabilidades técnicas, la organización debería considerar: a) definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de la vulnerabilidad, incluida la supervisión de la vulnerabilidad, la evaluación del riesgo de vulnerabilidad, la actualización, el seguimiento de los activos y las responsabilidades de coordinación necesarias; b) identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas, para el software y otras tecnologías (según la lista de inventario de activos, ver 5.9), al 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 del sistema de información (incluidos sus componentes) que garanticen la notificación, el tratamiento y la divulgación de vulnerabilidades, incluidos los requisitos de los contratos aplicables (ver 5.20); d) utilizar herramientas de análisis de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y comprobar si la aplicación de parches de vulnerabilidades se ha realizado correctamente; e) realizar pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles por parte de personas competentes y autorizadas para apoyar la identificación de vulnerabilidades. Actuar con cautela ya que tales actividades pueden conducir a un compromiso de la seguridad del sistema; f) realizar un seguimiento del uso de bibliotecas de terceros y del código fuente en busca de vulnerabilidades. Esto debería ser incluido en la codificación segura (ver 8.28). La organización debería desarrollar procedimientos y capacidades para: a) detectar la existencia de vulnerabilidades en sus productos y servicios, incluido cualquier componente externo utilizado en ellos; b) recibir informes de vulnerabilidad de fuentes internas o externas. La organización debería proporcionar un punto de contacto público como parte de una política específica de temas sobre la divulgación de la vulnerabilidad para que los investigadores y otras personas puedan informar de los problemas. La organización debería establecer procedimientos de notificación de vulnerabilidades, formularios de presentación de informes en línea y hacer uso de la inteligencia de amenazas apropiada o foros de intercambio de información. La organización también debería considerar programas de recompensa de errores donde se ofrecen 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 industriales competentes u otras partes interesadas. **Evaluación de vulnerabilidades técnicas** Para evaluar las vulnerabilidades técnicas identificadas, se debería tener en cuenta la siguiente guía: a) analizar y verificar los informes para determinar qué respuesta y actividad de corrección son necesarias; b) una vez identificada una posible vulnerabilidad técnica, se identifican los riesgos asociados y las medidas que se deberían tomar. Estas acciones pueden implicar la actualización de sistemas vulnerables o la aplicación de otros controles. **Tomar las medidas adecuadas para abordar las vulnerabilidades técnicas**

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Se debería implementar un proceso de gestión de actualizaciones de software para garantizar que se instalan los parches y actualizaciones de aplicaciones aprobados más actualizados para todo el software autorizado. Si es necesario realizar cambios, se debería conservar el software original y aplicar los cambios a una copia designada. Todos los cambios deberían probarse y documentarse por completo, de modo que se puedan volver a aplicar, si es necesario, a futuras actualizaciones de software. Si es necesario, las modificaciones deberían ser probadas y validadas por un organismo de evaluación independiente. Se debería tener en cuenta la siguiente guía para abordar las vulnerabilidades técnicas: a) adoptar medidas apropiadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un calendario para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes; b) dependiendo de la urgencia con que se deba abordar una vulnerabilidad técnica, llevar a cabo la acción de acuerdo con los controles relacionados con la gestión de cambios (ver 8.32) o siguiendo los procedimientos de respuesta a incidentes de SI (ver 5.26); c) utilizar solo actualizaciones de fuentes legítimas (que pueden ser internas o externas a la organización); d) probar y evaluar las actualizaciones antes de instalarlas para asegurarse de que son efectivas y no producen efectos secundarios que no se pueden tolerar (es decir, si hay una actualización disponible, evaluando los riesgos asociados con la instalación de la actualización (los riesgos que plantea la vulnerabilidad deberían compararse con el riesgo de instalar la actualización)); e) abordar primero los sistemas de alto riesgo; f) desarrollar soluciones (normalmente actualizaciones de software o parches); g) probar para confirmar si la remediación o mitigación es efectiva; h) proporcionar mecanismos para verificar la autenticidad de la corrección; i) revisar si no hay ninguna actualización disponible o la actualización no se puede instalar, tomando en consideración otros controles, como: 1) aplicar cualquier solución sugerida por el proveedor del software u otras fuentes relevantes; 2) desactivar servicios o capacidades relacionados con la vulnerabilidad; 3) adaptar o añadir controles de acceso (por ejemplo, firewalls) en los límites de la red (ver 8.20 a 8.22); 4) proteger sistemas, dispositivos o aplicaciones vulnerables frente a ataques mediante la implementación de filtros de tráfico adecuados (a veces denominados parches virtuales); 5) aumentar la supervisión para detectar ataques reales; 6) sensibilizar sobre la vulnerabilidad. En el caso del software adquirido, si los proveedores regularmente liberan información sobre las actualizaciones de seguridad de su software y proporcionan una instalación para instalar dichas actualizaciones automáticamente, la organización debería decidir si se debería utilizar o no la actualización automática. **Otras consideraciones** Se debería mantener un registro de auditoría para todos los pasos emprendidos en la gestión técnica de vulnerabilidades. El proceso de gestión de la vulnerabilidad técnica debería ser supervisado y evaluado periódicamente para asegurar su eficacia y eficiencia. Un proceso de gestión de vulnerabilidad técnica eficaz debería estar alineado con las actividades de gestión de incidentes, para comunicar datos sobre vulnerabilidades a la función de respuesta a incidentes y proporcionar procedimientos técnicos que se deberían llevar a cabo en caso de que se produzca un incidente. Cuando la organización utiliza un servicio en la nube proporcionado por un proveedor de servicios en la nube de terceros, éste debería garantizar la gestión de vulnerabilidades técnicas de los recursos y servicios del provistos la nube. Las responsabilidades del proveedor de servicios en la nube para la gestión de vulnerabilidades técnicas deberían formar parte del acuerdo de servicios en la nube y esto debería incluir procesos para informar de las acciones del proveedor de servicios en la nube relacionadas con vulnerabilidades técnicas (ver 5.23). Para algunos servicios en la nube, existen responsabilidades respectivas para el proveedor de servicios en la nube y el cliente de servicios en la nube. Por ejemplo, el cliente del servicio en la nube es responsable de la gestión de vulnerabilidades de sus propios activos utilizados para los servicios en la nube.

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

OTRA INFORMACIÓN	La gestión técnica de la vulnerabilidad puede considerarse una subfunción de la gestión del cambio y, como tal, puede aprovechar los procesos y procedimientos de gestión del cambio (ver 8.32). Existe la posibilidad de que una actualización no aborde el problema adecuadamente y tenga efectos secundarios negativos. Además, en algunos casos, la desinstalación de una actualización no se puede realizar fácilmente una vez aplicada la actualización. Si no es posible realizar pruebas adecuadas de las actualizaciones (por ejemplo, debido a los costos o a la falta de recursos), se puede considerar un retraso en la actualización para evaluar los riesgos asociados, en función de la experiencia reportada por otros usuarios. El uso de la norma ISO/IEC 27031 puede ser beneficioso. Cuando se produzcan parches o actualizaciones de software, la organización puede considerar la posibilidad de proporcionar un proceso de actualización automatizado en el que estas actualizaciones se instalen en los sistemas o productos afectados sin necesidad de intervención del cliente o del usuario. Si se ofrece un proceso de actualización automatizado, puede permitirle al cliente o usuario elegir una opción para desactivar la actualización automática o controlar el momento de la instalación de la actualización. Cuando el proveedor proporciona un proceso de actualización automatizado y las actualizaciones se pueden instalar en los sistemas o productos afectados sin necesidad de intervención, la organización determina si aplica o no el proceso automatizado. Una razón por la que no se elige la actualización automática es mantener el control cuando se realiza la actualización. Por ejemplo, un software utilizado para una operación de negocio no se puede actualizar hasta que la operación se haya completado. Un punto débil del análisis de vulnerabilidades es que es posible que no tenga en cuenta completamente la defensa en profundidad: Dos contramedidas que siempre se invocan en secuencia pueden tener vulnerabilidades enmascaradas por puntos fuertes en la otra. La medida compensada compuesta no es vulnerable, mientras que un analizador de vulnerabilidades puede informar de que ambos componentes son vulnerables. Por lo tanto, la organización debería tener cuidado al examinar y actuar en relación con los informes de vulnerabilidad. Muchas organizaciones suministran software, sistemas, productos y servicios no solo dentro de la organización, sino también a partes interesadas como clientes, socios u otros usuarios. Este software, sistemas, productos y servicios pueden tener vulnerabilidades de SI que afectan a la seguridad de los usuarios. Las organizaciones pueden publicar soluciones y divulgar información sobre vulnerabilidades a los usuarios (normalmente a través de un asesoramiento público) y proporcionar información adecuada para los servicios de base de datos de vulnerabilidades de software. Más información sobre la gestión de vulnerabilidades técnicas al utilizar computación en la nube en las series ISO/IEC 19086 e ISO/IEC 27017. La norma ISO/IEC 29147 proporciona información detallada sobre la recepción de informes y la publicación de alertas de vulnerabilidad. La norma ISO/IEC 30111 proporciona información detallada sobre el manejo y la resolución de vulnerabilidades reportadas.

8.9. GESTIÓN DE LA CONFIGURACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Configuración_segura**	**#Protección**	**Nuevo**
CONTROL	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deberían establecer, documentar, implementar, supervisar y revisar.					
PROPÓSITO	Para garantizar que el hardware, el software, los servicios y las redes funcionan correctamente con la configuración de seguridad requerida y la configuración no se ve alterada por cambios no autorizados o incorrectos.					
ORIENTACIÓN	**General** La organización debería definir e implementar procesos y herramientas para aplicar las configuraciones definidas (incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para sistemas recién instalados y para sistemas operativos a lo largo de su vida útil. Deberían establecerse funciones, responsabilidades y procedimientos para garantizar un					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	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) al utilizar orientaciones disponibles públicamente (por ejemplo, plantillas predefinidas de proveedores y de organizaciones de seguridad independientes); b) al considerar el nivel de protección necesario para determinar un nivel suficiente de seguridad; c) al apoyar la política de SI de la organización, a las políticas de temas específicos, a las normas y a otros requisitos de seguridad; d) al considerar la viabilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización. Las plantillas deberían revisarse periódicamente y actualizarse cuando sea necesario abordar nuevas amenazas o vulnerabilidades o cuando se introduzcan nuevas versiones de software o hardware. Se debería tener en cuenta lo siguiente para establecer plantillas estándar para la configuración segura de hardware, software, servicios y redes: a) minimizar el número de identidades con derechos de acceso a nivel de administrador o con privilegios; b) deshabilitar identidades innecesarias, no utilizadas o inseguras; c) deshabilitar o restringir funciones y servicios innecesarios; d) restringir el acceso a potentes programas utilitarios y a la configuración de parámetros de host; e) sincronizar los relojes; f) cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad predeterminada; g) invocar las funciones de tiempo de espera que desconectan automáticamente los dispositivos informáticos después de un período predeterminado de inactividad; h) verificar que se han cumplido los requisitos de licencia (ver 5.32). **Gestión de configuraciones** Se deberían registrar las configuraciones establecidas de hardware, software, servicios y redes y se debería mantener un registro de todos los cambios de configuración. Estos registros deberían almacenarse de forma segura. Esto se puede lograr de varias maneras, como bases de datos de configuración o plantillas de configuración. Los cambios en las configuraciones deberían seguir el proceso de administración de cambios (ver 8.32). Los registros de configuración pueden contener, según corresponda: a) información actualizada del propietario o punto de contacto del activo; b) fecha del último cambio de configuración; c) versión de la plantilla de configuración; d) relación con las configuraciones de otros activos. Configuraciones de monitoreo. Las configuraciones deberían monitorearse con un conjunto completo de herramientas de administración del sistema (por ejemplo, servicios de mantenimiento, soporte remoto, herramientas de administración de la empresa, software de copia de seguridad y restauración) y deberían revisarse periódicamente para verificar la configuración, evaluar la intensidad de la contraseña y evaluar las actividades realizadas. Las configuraciones reales se pueden comparar con las plantillas de destino definidas. Cualquier desviación debería ser tratada ya sea mediante la aplicación automática de la configuración de blanco definida o mediante el análisis manual de la desviación seguida de acciones correctivas.
OTRA INFORMACIÓN	La documentación de los sistemas suele registrar detalles sobre la configuración tanto del hardware como del software. El endurecimiento del sistema (hardening) es una parte representativa de la gestión de la configuración. La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas. La automatización suele ser más eficaz para gestionar la configuración de la seguridad (por ejemplo, al utilizar la infraestructura como código). Las plantillas de configuración y los destinos pueden ser información confidencial y deberían protegerse del acceso no autorizado en consecuencia.

8.10. ELIMINACIÓN DE INFORMACIÓN

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad**	**#Proteger**	**#Protección_de_la_información #Legal_y_cumplimiento**	**#Protección**	**Nuevo**
CONTROL	La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento debería eliminarse cuando ya no sea necesario.					
PROPÓSITO	Evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, legales, reglamentarios y contractuales para la eliminación de información.					
ORIENTACIÓN	**General** La información confidencial no debería conservarse durante más tiempo del necesario para reducir el riesgo de divulgación indeseable. Al eliminar información sobre sistemas, aplicaciones y servicios, se debería tener en cuenta lo siguiente: a) seleccionar un método de borrado (por ejemplo, sobreescritura electrónica o borrado cifrado) de acuerdo con los requisitos de la empresa y tomando en consideración las leyes y reglamentos pertinentes; b) registrar los resultados de la eliminación como prueba; c) obtener pruebas de la eliminación de dicha información, cuando se utilicen proveedores de servicios de eliminación de información. Cuando terceros almacenen la información de la organización en su nombre, la organización debería considerar la inclusión de requisitos sobre la eliminación de información en los acuerdos de terceros para aplicarla durante y al terminar dichos servicios. **Métodos de eliminación** De conformidad con la política temática específica de la organización sobre la retención de datos y tomando en consideración la legislación y los reglamentos pertinentes, la información confidencial debería eliminarse cuando ya no sea necesaria mediante: a) configuración de sistemas para destruir información de forma segura cuando ya no sea necesaria (por ejemplo, después de un período definido sujeto a la política específica del tema sobre la retención de datos o por solicitud de acceso del sujeto); b) eliminación de versiones obsoletas, copias y archivos temporales dondequiera que se encuentren; c) uso de software de eliminación seguro aprobado para eliminar información de forma permanente para garantizar que la información no se pueda recuperar mediante herramientas forenses o de recuperación especializada; d) uso de proveedores autorizados y certificados de servicios de eliminación segura; e) uso de mecanismos de eliminación adecuados para el tipo de medio de almacenamiento que se va a desechar (por ejemplo, desmagnetización de unidades de disco duro y otros medios de almacenamiento magnético). Cuando se utilizan servicios en la nube, la organización debería comprobar si el método de eliminación proporcionado por el proveedor de servicios en la nube es aceptable y, en caso afirmativo, la organización debería utilizarlo o solicitar que el proveedor de servicios en la nube elimine la información. Estos procesos de eliminación se deberían automatizar de acuerdo con las políticas específicas del tema, cuando estén disponibles y sean aplicables. En función de la sensibilidad de la información eliminada, los registros pueden realizar un seguimiento o verificar que se han producido estos procesos de eliminación. Para evitar la exposición accidental de información confidencial cuando el equipo se regresa a los proveedores, la información confidencial debería protegerse eliminando almacenamientos auxiliares (por ejemplo, unidades de disco duro) y la memoria antes de que el equipo salga de las instalaciones de la organización. Tomando en consideración que la eliminación segura de algunos dispositivos (por ejemplo, smartphones) solo se puede lograr mediante la destrucción o el uso de las funciones integradas en estos dispositivos (por ejemplo “restaurar ajustes de fábrica”), la organización debería elegir el método apropiado de acuerdo con la clasificación de la información que manejan dichos dispositivos. Las medidas de control descritas en 7.14 deberían aplicarse para destruir físicamente el dispositivo de almacenamiento y eliminar simultáneamente la información que contiene. Un registro oficial de eliminación de información es útil al analizar la causa de un posible evento de fuga de información.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

OTRA INFORMACIÓN	La información sobre la eliminación de datos de usuario en los servicios en la nube se encuentra en la ISO/IEC 27017. En la norma ISO/IEC 27555 se puede encontrar información sobre la eliminación de la IIP.

8.11. ENMASCARAMIENTO DE DATOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad**	**#Proteger**	**#Protección_de_la_información**	**#Protección**	**Nuevo**
CONTROL	El enmascaramiento de datos debería utilizarse de acuerdo con la política de la organización sobre el control de acceso y otras políticas específicas de temas relacionados, así como con los requisitos empresariales, tomando en consideración la legislación aplicable.					
PROPÓSITO	Limitar la exposición de datos sensibles, incluida la IIP y cumplir con los requisitos legales, estatutario, reglamentarios y contractuales.					
ORIENTACIÓN	Cuando la protección de datos sensibles (por ejemplo, IIP) es una preocupación, la organización debería considerar la posibilidad de ocultar tales datos mediante técnicas como el enmascaramiento de datos, la pseudoanonimizados o la anonimización. Las técnicas de pseudoanonimización o anonimización pueden ocultar la IIP, ocultar la verdadera identidad de los dueños de la IIP u otra información sensible y desconectar el vínculo entre la IIP y la identidad del titular de la IIP o el vínculo con otra información sensible. Cuando se utilicen técnicas de pseudoanonimización o anonimización, debería verificarse que los datos han sido adecuadamente pseudoanonimizados o anonimizados. La anonimización de los datos debería considerar que todos los elementos de la información confidencial son eficaces. Por ejemplo, si no se considera adecuadamente, una persona puede ser identificada, aunque los datos que pueden identificarla directamente sean anónimos, por la presencia de otros datos que permiten identificarla indirectamente. Entre las técnicas adicionales para el enmascaramiento de datos se incluyen: a) cifrado (que requiere que los usuarios autorizados tengan una clave); b) anular o eliminar caracteres (impedir que los usuarios no autorizados vean mensajes completos); c) números y fechas variables; d) sustitución (cambiar un valor por otro para ocultar datos confidenciales); e) reemplazar valores con su hash. Al implementar técnicas de enmascaramiento de datos, se debería tener en cuenta: a) no conceder a todos los usuarios acceso a todos los datos, por lo tanto, diseñar consultas y máscaras para mostrar solo los datos mínimos necesarios para el usuario; b) hay casos en los que algunos datos no deberían ser visibles al usuario para algunos registros de un conjunto de datos; en este caso, diseñar e implementar un mecanismo de ofuscación de datos (por ejemplo, si un paciente no quiere que el personal del hospital pueda ver todos sus historiales, incluso en caso de emergencia, entonces el personal del hospital se presenta con datos parcialmente ofuscados y solo puede acceder a los datos el personal con roles específicos si contiene información útil para el tratamiento adecuado); c) cuando los datos están ofuscados, lo que da al titular de la IIP la posibilidad de exigir que los usuarios no puedan ver si los datos están enmascarados (ocultación del enmascaramiento; esto se utiliza en los centros de salud, por ejemplo, si el paciente no desea que el personal vea que se ha ocultado información sensible como embarazos o resultados de exámenes de sangre); d) cualquier requisito legal o reglamentario (por ejemplo, que requiera el enmascaramiento de la información de las tarjetas de pago durante el procesamiento o almacenamiento). A la hora de utilizar el enmascaramiento, la pseudoanonimización o la anonimización de los datos debería tenerse en cuenta lo siguiente: a) nivel de intensidad del enmascaramiento de datos, pseudoanonimización o anonimización según el uso de los datos procesados; b) controles de acceso a los datos procesados; c) acuerdos o restricciones sobre el uso de los datos procesados; d) la imposibilidad de cotejar los datos procesados con otra información para identificar al titular de la IIP;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	e) realizar un seguimiento de la provisión y recepción de los datos procesados.
OTRA INFORMACIÓN	La anonimización altera irreversiblemente la IIP de tal manera que el titular de la IIP ya no puede identificarse directa o indirectamente. La pseudoanonimización sustituye la información de identificación por un alias. El conocimiento del algoritmo (en ocasiones denominado "información adicional") utilizado para realizar la pseudoanonimización permite al menos alguna forma de identificación del titular de la IIP. Por consiguiente, esa "información adicional" debería mantenerse separada y protegida. Mientras que la pseudoanonimización es, por lo tanto, más débil que la anonimización, los conjuntos de datos pseudoanonimizados pueden ser más útiles en la investigación estadística. El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ocultar elementos de datos confidenciales. El enmascaramiento de datos puede ser estático (cuando los elementos de datos están enmascarados en la base de datos original), dinámico (mediante automatización y reglas para proteger los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación). Las funciones hash se pueden utilizar para convertir en anónima la IIP. Con el fin de evitar los ataques de enumeración, siempre deberían combinarse con una función "Salt". La IIP en los identificadores de recursos y sus atributos (por ejemplo, nombres de archivo, localizadores de recursos uniformes (URL)) se debería evitar o se debería anonimizar de forma adecuada. En la norma ISO/IEC 27018 se ofrecen controles adicionales sobre la protección de la IIP en las nubes públicas

8.12. PREVENCIÓN DE FUGA DE DATOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo #Detectivo	**#Confidencialidad**	**#Proteger #Detectar**	**#Protección_de_la_información**	**#Protección**	**Nuevo**
CONTROL	Las medidas de prevención de fugas de datos deberían aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.					
PROPÓSITO	Detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.					
ORIENTACIÓN	La organización debería considerar lo siguiente para reducir el riesgo de fuga de datos: a) identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos); b) supervisar los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles); c) actuar para evitar que se filtre información (por ejemplo, correos electrónicos de cuarentena que contengan información confidencial). Se deberían utilizar herramientas de prevención de fugas de datos para: a) identificar y supervisar la información confidencial en riesgo de divulgación no autorizada (por ejemplo, en datos no estructurados del sistema de un usuario); b) detectar la divulgación de información confidencial (por ejemplo, cuando la información se carga en servicios en la nube de terceros que no son de confianza o se envía por correo electrónico); c) bloquear las acciones de los usuarios o las transmisiones de red que exponen información confidencial (por ejemplo, impedir la copia de entradas de la base de datos en una hoja de cálculo). La organización debería determinar si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización. Si ese es el caso, la organización debería implementar tecnología como herramientas de prevención de fugas de datos o la configuración de herramientas existentes que permitan a los usuarios ver y manipular los datos almacenados de forma remota, pero que impidan la copia y el pegado fuera del control de la organización. Si se requiere la exportación de datos, se debería permitir al propietario de los datos aprobar la exportación y hacer que los usuarios sean responsables de sus acciones. La realización de capturas de pantalla o fotografías de la pantalla debería abordarse mediante los términos y condiciones de uso, formación y auditoría.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Cuando se realiza una copia de seguridad de los datos, se debería tener cuidado de garantizar la protección de la información confidencial mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad. La prevención de fugas de datos también debería considerarse para proteger contra las acciones de inteligencia de un adversario de la obtención de información confidencial o secreta (geopolítica, humana, financiera, comercial, científica o de cualquier otra índole) que pueda ser de interés para el espionaje o puede ser crítica para la comunidad. Las acciones de prevención de fugas de datos deberían orientarse a confundir las decisiones del adversario, por ejemplo, sustituyendo la información auténtica por información falsa ya sea como una acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de "honeypots" para atraer atacantes.

8.13. COPIAS DE SEGURIDAD DE LA INFORMACIÓN (RESPALDOS)

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Correctivo	**#Integridad #Disponibilidad**	**#Recuperar**	**#Continuidad**	**#Protección**	**12.3.1**
CONTROL	Las copias de seguridad (respaldos) de la información, del software y de los sistemas deberían mantenerse y probarse periódicamente de conformidad con una política de copias de seguridad específica acordada.					
PROPÓSITO	Permitir la recuperación de la pérdida de datos o sistemas.					
ORIENTACIÓN	Se debería establecer una política de copia de seguridad específica para abordar los requisitos de retención de datos y SI de la organización. Se deberían proporcionar las instalaciones de copia de seguridad adecuadas para garantizar que toda la información y el software esenciales se puedan recuperar tras un incidente, falla o pérdida de los medios de almacenamiento. Se deberían desarrollar e implementar planes para la forma en que la organización realizará copias de seguridad, el software y los sistemas, para abordar la política específica del tema sobre copias de seguridad. Al diseñar un plan de copias de seguridad, se deberían tener en cuenta los siguientes elementos: a) producir registros precisos y completos de las copias de seguridad y procedimientos de restauración documentados; b) reflejar los requisitos de la organización (por ejemplo, el objetivo del punto de recuperación, ver 5.30), los requisitos de SI implicada y la importancia de la información para el funcionamiento continuo de la organización en la medida (por ejemplo, copia de seguridad completa o diferencial) y la frecuencia de las copias de seguridad; c) almacenar las copias de seguridad en una ubicación remota segura y a una distancia suficiente para evitar cualquier daño causado por un desastre en el sitio principal; d) proporcionar a la información de copia de seguridad un nivel adecuado de protección física y ambiental (ver la Cláusula 7 y 8.1) coherente con las normas aplicadas en el sitio principal; e) probar regularmente los medios de copia de seguridad para garantizar que se pueden confiar en ellos para su uso de emergencia cuando sea necesario. Probar la capacidad de restaurar los datos de copia de seguridad en un sistema de prueba, no sobrescribiendo los medios de almacenamiento originales en caso de que el proceso de copia de seguridad o restauración falle y cause daños o pérdidas irreparables en los datos; f) proteger las copias de seguridad mediante cifrado de acuerdo con los riesgos identificados (por ejemplo, en situaciones en las que la confidencialidad es importante); g) asegúrese de que se detecte una pérdida de datos inadvertida antes de realizar la copia de seguridad. Los procedimientos operativos deberían supervisar la ejecución de las copias de seguridad y solucionar las fallas de las copias de seguridad programadas para garantizar la integridad de las copias de seguridad de acuerdo con la política de copias de seguridad específica del tema. Las medidas de respaldo para sistemas y servicios individuales deberían ser probadas regularmente para asegurar que cumplen con los PROPÓSITOS de respuesta a incidentes y					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	planes de continuidad del negocio (ver 5.30). Esto debería combinarse con una prueba de los procedimientos de restauración y verificarse 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 abarcar toda la información, las aplicaciones y los datos de los sistemas necesarios para recuperar todo el sistema en caso de desastre. Cuando la organización utiliza un servicio en la nube, se deberían realizar copias de SI, las aplicaciones y los sistemas de la organización en el entorno del servicio en la nube. La organización debería determinar si se cumplen los requisitos de copia de seguridad y cómo se cumplen al utilizar el servicio de copia de seguridad de información proporcionado como parte del servicio en la nube. Se debería determinar el período de retención de la información empresarial esencial, tomando en consideración cualquier requisito de retención de copias archivadas. La organización debería considerar la eliminación de información (ver 8.10) en los medios de almacenamiento utilizados para la copia de seguridad una vez que el período de retención de la información expire y debería tener en cuenta la legislación y las regulaciones.
OTRA INFORMACIÓN	Más información sobre la seguridad del almacenamiento, incluida la consideración de la retención en la norma ISO/IEC 27040.

8.14. REDUNDANCIA DE LAS INSTALACIONES DE TRATAMIENTO DE INFORMACIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Disponibilidad**	**#Proteger**	**#Continuidad #Gestión_de_activos**	**#Protección #Resilencia**	**17.2.1**
CONTROL	Las instalaciones de procesamiento de información deberían implementarse con redundancia suficiente para satisfacer los requisitos de disponibilidad.					
PROPÓSITO	Garantizar el funcionamiento continuo de las instalaciones de procesamiento de información.					
ORIENTACIÓN	La organización debería identificar los requisitos para la disponibilidad de servicios organizacionales y sistemas de información. La organización debería diseñar e implementar una arquitectura de sistemas con redundancia adecuada para satisfacer estos requisitos. La redundancia se puede introducir duplicando las instalaciones de procesamiento de información en parte o en su totalidad (por ejemplo, componentes de repuesto o tener dos de todo). La organización debería planificar e implementar procedimientos para la activación de los componentes redundantes y las instalaciones de procesamiento. Los procedimientos deberían establecer si los componentes redundantes y las actividades de procesamiento siempre están activados o en caso de emergencia, se activan automática o manualmente. Los componentes redundantes y las instalaciones de procesamiento de la información deberían garantizar el mismo nivel de seguridad que los principales. Deberían existir mecanismos para alertar a la organización de cualquier falla en las instalaciones de procesamiento de información, permitir la ejecución del procedimiento planificado y permitir una disponibilidad continua mientras se reparan o reemplazan las instalaciones de procesamiento de información. La organización debería tener en cuenta lo siguiente al implementar sistemas redundantes: a) contratar con dos o más proveedores de redes e instalaciones de procesamiento de información crítica, como proveedores de servicios de internet; b) uso de redes redundantes; c) utilizar dos centros de datos separados geográficamente con sistemas duplicados; d) uso de fuentes de energía o fuentes físicamente redundantes; e) utilizar varias instancias paralelas de componentes de software, con equilibrio de carga automático entre ellos (entre instancias en el mismo centro de datos o en diferentes centros de datos); f) tener componentes duplicados en los sistemas (por ejemplo, CPU, discos duros, memorias) o en redes (por ejemplo, firewalls, routers, switches). Cuando sea aplicable, preferiblemente en modo de producción, se deberían probar sistemas de información redundantes para garantizar que la conmutación por error de un componente a otro funciona según lo previsto.					
OTRA INFORMACIÓN	Existe una fuerte relación entre la redundancia y la preparación de las TIC para la continuidad del negocio (ver 5.30), especialmente si se requieren tiempos de recuperación cortos.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	Muchas de las medidas de redundancia pueden formar parte de las estrategias y soluciones de continuidad de las TIC. La implementación de redundancias puede generar riesgos para la integridad (por ejemplo, los procesos de copia de datos en componentes duplicados pueden introducir errores) o la confidencialidad (por ejemplo, un control débil de la seguridad de los componentes duplicados puede llevar a un compromiso) de los sistemas de información y de información, que deberían tenerse en cuenta al diseñar sistemas de información. La redundancia en las instalaciones de procesamiento de información normalmente no aborda la indisponibilidad de las aplicaciones debido a fallas dentro de una aplicación. Con el uso de computación en la nube pública, es posible disponer de varias versiones en directo de las instalaciones de procesamiento de información, que existen en varias ubicaciones físicas independientes con failover automático (o conmutación por error) y equilibrio de carga entre ellas. Algunas de las tecnologías y técnicas para proporcionar redundancia y failover automático en el contexto de los servicios en la nube se analizan en la ISO/IEC TS 23167.

8.15. REGISTROS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Detectivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Detectar**	**#Gestión_de_eventos_deSI**	**#Protección #Defensa**	**12.4.1 12.4.2 12.4.3**
CONTROL	Deberían producirse, almacenarse, protegerse y analizarse los registros que recogen las actividades, las excepciones, los fallas y otros eventos relevantes.					
PROPÓSITO	Para registrar eventos, generar pruebas, garantizar la integridad de la información de registro, evitar el acceso no autorizado, identificar eventos de SI que pueden dar lugar a un incidente de SI y respaldar las investigaciones.					
ORIENTACIÓN	**General** La organización debería determinar el objetivo para el que se crean los registros, los datos que se recopilan y registran y los requisitos específicos para proteger y gestionar los datos del registro. Esto debería documentarse en una directiva 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 los eventos relevantes (por ejemplo, inicio y cierre de sesión); d) identidad del dispositivo, identificador del sistema y ubicación; e) direcciones de red y protocolos. Los siguientes eventos deberían ser considerados para el registro: a) intentos de acceso al sistema exitosos y rechazados; b) datos correctos y rechazados y otros intentos de acceso a recursos; c) cambios en la configuración del sistema; d) uso de privilegios; e) uso de programas y aplicaciones utilitarios; f) los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes; g) alarmas generadas 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 eliminación de identidades; j) transacciones ejecutadas por usuarios en aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o ejecutado por un tercero. Es importante que todos los sistemas tengan orígenes de tiempo sincronizados (ver 8.17) ya que esto permite la correlación de registros entre sistemas para el análisis, las alertas y la investigación de un incidente. **Protección de registros** Los usuarios, incluidos aquellos con derechos de acceso privilegiado, no deberían tener permiso para eliminar o desactivar registros de sus propias actividades. Pueden manipular potencialmente los registros de las instalaciones de procesamiento de información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	responsabilidad de los usuarios con privilegios. Los controles deberían tener como objetivo proteger contra cambios no autorizados en la información de registro y problemas operativos con la instalación de registro, incluidos: a) modificaciones de los tipos de mensajes que se graban; b) archivos de registro que se están editando o eliminando; c) error al grabar eventos o sobreescritura de eventos grabados pasados si se excede el medio de almacenamiento que contiene un archivo de registro. Para la protección de registros, se debería considerar el uso de las siguientes técnicas: Hash de cifrado, grabación en un archivo de solo anexión y de solo lectura, grabación en un archivo de transparencia pública. Algunos registros de auditoría pueden ser necesarios para archivarse debido a los requisitos de retención de datos o a los requisitos para recopilar y conservar pruebas (ver 5.28). Cuando la organización necesite enviar registros del sistema o de la aplicación a un proveedor para ayudar con la depuración o la solución de errores, los registros deberían desidentificarse siempre que sea posible mediante técnicas de enmascaramiento de datos (ver 8.11) para obtener información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlos al proveedor. Los registros de eventos pueden contener datos confidenciales e información de identificación personal. Deberían adoptarse medidas adecuadas de protección de la intimidad (ver 5.34). **Análisis de registros** El análisis de los registros debería abarcar el análisis y la interpretación de los eventos de SI, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso. El análisis de los eventos debería realizarse tomando en consideración: a) las habilidades necesarias para los expertos que realizan el análisis; b) el procedimiento de análisis de los registros; c) los atributos necesarios de cada evento relacionado con la seguridad; d) 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 malware); e) patrones de comportamiento conocidos y tráfico de red estándar en comparación con la actividad y el comportamiento anómalos (análisis de comportamiento de usuarios y entidades (UEBA)); f) resultados del análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de big data y herramientas de análisis especializadas); g) inteligencia de amenazas disponible. El análisis de los registros debería estar respaldado por actividades de supervisión específicas para ayudar a identificar y analizar el comportamiento anómalo, que incluye: a) revisar los intentos correctos e incorrectos de acceder a los recursos protegidos (por ejemplo, servidores del sistema de nombres de dominio (DNS), portales web y recursos compartidos de archivos); b) comprobar los registros DNS para identificar las conexiones de red salientes a servidores malintencionados, como los asociados a los servidores de control y comandos botnet; c) examinar los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicio) para determinar si hay actividad inusual en los sistemas y las redes (por ejemplo, revisando los patrones de actividad); d) incluir registros de eventos de monitoreo físico, como entrada y salida, para garantizar una detección y análisis de incidentes más precisos; e) correlacionar registros para permitir un análisis eficiente y muy preciso. Los incidentes de SI sospechosos y reales deberían identificarse (por ejemplo, infección por malware o sondeo de firewalls) y estar sujetos a una investigación más exhaustiva (por ejemplo, como parte de un proceso de gestión de incidentes de SI, ver 5.25).
OTRA INFORMACIÓN	Los registros del sistema suelen contener un gran volumen de información, gran parte de la cual es ajena a la supervisión de la SI. Para ayudar a identificar eventos significativos con fines de supervisión de la SI, se puede considerar el uso de programas utilitarios o herramientas de auditoría adecuados para realizar la interrogación de archivos. El registro de eventos sienta las bases de los sistemas de supervisión automatizados (ver 8.16), que son capaces de generar informes consolidados y alertas sobre la seguridad del sistema.

	Se puede utilizar una herramienta SIEM (Security Incident Event Management) o un servicio equivalente para almacenar, correlacionar, normalizar y analizar la información de registro, así como para generar alertas. Los SIEM tienden a requerir una configuración cuidadosa para optimizar sus beneficios. Las configuraciones a considerar incluyen identificación y selección de fuentes de registro apropiadas, ajuste y prueba de reglas y desarrollo de casos de uso. Los archivos de transparencia pública para el registro de registros se utilizan, por ejemplo, en sistemas de transparencia de certificados. Estos archivos pueden proporcionar un mecanismo de detección adicional útil para proteger contra la manipulación de registros. En los entornos de nube, las responsabilidades de gestión de registros se pueden compartir entre el cliente del servicio de nube y el proveedor de servicios de nube. Las responsabilidades varían en función del tipo de servicio en la nube que se utilice. Más información en la norma ISO/IEC 27017.

8.16. ACTIVIDADES DE MONITOREO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Detectivo #Corrección	**#Confidencialidad #Integridad #Disponibilidad**	**#Detectar #Responder**	**#Gestión_de_eventos_de_SI**	**#Defensa**	**Nuevo**
CONTROL	Las redes, los sistemas y las aplicaciones deberían ser monitoreados para detectar comportamientos anómalos y tomar las medidas apropiadas para evaluar posibles incidentes de SI.					
PROPÓSITO	Detectar comportamientos anómalos y posibles incidentes de SI.					
ORIENTACIÓN	El alcance y el nivel de supervisión deberían determinarse de conformidad con los requisitos de seguridad de la organización y la información y tomando en consideración las leyes y reglamentos pertinentes. Los registros de supervisión deberían mantenerse para los períodos de retención definidos. Se debería considerar la inclusión de los siguientes elementos en el sistema de supervisión: a) tráfico de red, sistema y aplicaciones salientes y entrantes; b) acceso a sistemas, servidores, equipos de red, sistema de supervisión, aplicaciones críticas, etc.; c) archivos de configuración del sistema y de la red de nivel crítico o administrativo; 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 se ha manipulado (por ejemplo, mediante recompilación para añadir 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 vigilar contra esta línea de base para detectar anomalías. Al establecer una línea base, se debería tener en cuenta lo siguiente: a) revisar la utilización de los sistemas en períodos normales y máximos; b) hora habitual de acceso, ubicación del acceso, frecuencia de acceso para cada usuario o grupo de usuarios. El sistema de supervisión debería configurarse con respecto a la línea base establecida para identificar el comportamiento anómalo, como: a) terminación no planificada de procesos o aplicaciones; b) actividad normalmente asociada con malware o tráfico procedente de direcciones IP o dominios de red maliciosos conocidos (por ejemplo, los asociados con los servidores de comando y control de botnet); 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, colas de red, niveles de latencia y fluctuación de red); f) acceso no autorizado (real o tentativo) a sistemas o información; f) análisis no autorizado de aplicaciones, sistemas y redes empresariales;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	g) intentos correctos e incorrectos de acceder a los recursos protegidos (por ejemplo, servidores DNS, portales web y recursos compartidos de archivos); h) comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado. Se debería utilizar el monitoreo continuo a través de una herramienta de monitoreo. El monitoreo debería realizarse en tiempo real o en intervalos periódicos, sujeto a las necesidades y capacidades de la organización. Las herramientas de supervisión deberían incluir la capacidad de gestionar 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 red o aplicaciones. El software de supervisión automatizada debería configurarse para generar alertas (por ejemplo, mediante consolas de administración, mensajes de correo electrónico o sistemas de mensajería instantánea) basándose en umbrales predefinidos. El sistema de alerta debería ser ajustado y entrenado en la línea de base de la organización para minimizar falsos positivos. El personal debería estar dedicado 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 eventos anormales deberían comunicarse a las partes relevantes para mejorar las siguientes actividades: Auditoría, evaluación de la seguridad, análisis y monitoreo de vulnerabilidades (ver 5.25). Deberían establecerse procedimientos para responder oportunamente a los indicadores positivos del sistema de vigilancia, a fin de minimizar el efecto de los eventos adversos (ver 5.26) en la SI. También deberían establecerse procedimientos para identificar y abordar falsos positivos, incluido el ajuste del software de supervisión para reducir el número de falsos positivos futuros.
OTRA INFORMACIÓN	La supervisión de la seguridad se puede mejorar mediante: a) Aprovechar los sistemas de inteligencia frente a amenazas (ver 5.7); b) Aprovechar las capacidades de aprendizaje automático e inteligencia artificial; c) Al utilizar listas de bloqueo o listas de permisos; d) Realizar una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ciberataques y ejercicios de respuesta cibernética) y utilizar los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable; e) Utilizar sistemas de supervisión del rendimiento para ayudar a establecer y detectar comportamientos anómalos; f) Aprovechar los registros en combinación con los sistemas de supervisión. Las actividades de supervisión se realizan a menudo al utilizar software especializado, como sistemas de detección de intrusiones. Se pueden configurar en una línea de base de las actividades normales, aceptables y esperadas del sistema y de la red. El monitoreo de comunicaciones anómalas ayuda a identificar botnets (es decir, un conjunto de dispositivos bajo el control malicioso del propietario de botnet, que se suele utilizar para montar ataques distribuidos de denegación de servicio en otros equipos de otras organizaciones). Si el equipo está controlado por un dispositivo externo, existe una comunicación entre el dispositivo infectado y el controlador. Por lo tanto, la organización debería emplear tecnologías para vigilar las comunicaciones anómalas y adoptar las medidas necesarias.

8.17. SINCRONIZACIÓN DE RELOJES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Detectivo	**#Integridad**	**#Proteger #Detectar**	**#Gestión_de_eventos_de_SI**	**#Protección #Defensa**	**12.4.3**
CONTROL	Los relojes de los sistemas de procesamiento de información utilizados por la organización deberían sincronizarse con las fuentes de tiempo aprobadas.					
PROPÓSITO	Permitir la correlación y el análisis de los eventos relacionados con la seguridad y otros datos registrados y apoyar las investigaciones sobre incidentes de SI.					
ORIENTACIÓN	Se deberían documentar e implementar los requisitos externos e internos de representación de tiempo, sincronización fiable y precisión. Tales requisitos pueden ser legales, legales, reglamentarios, contractuales, normativos y de control interno. Se debería definir y					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	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 en las investigaciones. Un reloj vinculado a un emisor de hora de radio desde un reloj atómico nacional o un sistema de posicionamiento global (GPS) debería utilizarse como reloj de referencia para los sistemas de registro; una fuente de fecha y hora coherente y fiable para garantizar la precisión de las marcas de hora (time stamp). Los protocolos como el protocolo de hora de red (NTP) o el protocolo de hora de precisión (PTP) deberían utilizarse para mantener todos los sistemas conectados en red sincronizados con un reloj de referencia. La organización puede utilizar dos fuentes de tiempo externas al mismo tiempo para mejorar la fiabilidad de los relojes externos y gestionar de forma adecuada cualquier variación. La sincronización del reloj puede ser difícil cuando se utilizan varios servicios en la nube o cuando se utilizan servicios en la nube y en las instalaciones. En este caso, se debería supervisar el reloj de cada servicio y registrar la diferencia para mitigar los riesgos derivados de las discrepancias.
OTRA INFORMACIÓN	La configuración correcta de los relojes de computador es importante para garantizar la precisión de los registros de eventos, que puede ser requerido para investigaciones o como evidencia en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar dichas investigaciones y dañar la credibilidad de dichas pruebas.

8.18. USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_deL_sistema_y_de_la_red #Configuración_segura #Seguridad_de_las_aplicaciones**	**#Protección**	**9.4.4**
CONTROL	El uso de programas utilitarios capaces de anular los controles del sistema y de las aplicaciones debería estar restringido y controlado de forma estricta.					
PROPÓSITO	Garantizar que el uso de programas utilitarios no perjudique los controles del sistema y de las aplicaciones para la SI.					
ORIENTACIÓN	Se deberían tener en cuenta las siguientes directrices para el uso de programas utilitarios que pueden ser capaces de anular los controles del sistema y de la aplicación: a) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados (Ver 8.2); b) usar procedimientos de identificación, autenticación y autorización para programas utilitarios, incluyendo la identificación única de la persona que utiliza los utiliza; c) definir y documentar los niveles de autorización para los programas utilitarios; d) autorizar el uso ad hoc de programas utilitarios; e) no poner los programas utilitarios a disposición de los usuarios que tengan acceso a las aplicaciones en sistemas donde se requiera la separación de tareas; f) eliminar o desactivar todos los programas utilitarios innecesarios; g) como mínimo, segregar de manera lógica los programas utilitarios del software de aplicación. Cuando sea práctico, separar las comunicaciones de red para dichos programas del tráfico de aplicaciones; h) limitar la disponibilidad de los programas utilitarios (por ejemplo, durante la duración de un cambio autorizado); i) registrar todo uso de programas utilitarios.					
OTRA INFORMACIÓN	La mayoría de los sistemas de información tienen uno o más programas utilitarios que pueden ser capaces de anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, backup y herramientas de red.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

8.19. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

ATRIBUTOS	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura #Seguridad_de_las_aplicaciones	#Protección	12.5.1 12.6.2
CONTROL	Deberían implementarse procedimientos y medidas para administrar de forma segura la instalación de software en sistemas operativos.					
PROPÓSITO	Garantizar la integridad de los sistemas operativos y evitar la explotación de las vulnerabilidades técnicas.					
ORIENTACIÓN	Se deberían tener en cuenta las siguientes directrices para gestionar de forma segura los cambios y la instalación del software en los sistemas operativos: a) realizar actualizaciones del software operativo solo por parte de administradores formados con la autorización de administración adecuada (ver 8.5); b) garantizar que solo se instala código ejecutable aprobado y ningún código de desarrollo o compiladores en los sistemas operativos; c) instalar y actualizar el software solo después de realizar pruebas exhaustivas y satisfactorias (ver 8.29 y 8.31); d) actualizar todas las bibliotecas de origen de programas correspondientes; e) utilizar un sistema de control de configuración para mantener el control de todo el software operativo, así como de la documentación del sistema; f) definir una estrategia de reversión (rollback) antes de implementar los cambios; g) mantener un registro de auditoría de todas las actualizaciones del software operativo; h) mantener un archivo de versiones antiguas de software, junto con toda la información y parámetros necesarios, procedimientos, detalles de configuración y software de soporte como medida de contingencia y durante el tiempo que el software sea necesario para leer o procesar datos archivados. Cualquier decisión de actualizar a una nueva versión debería tener en cuenta los requisitos organizacionales para el cambio y la seguridad de la versión (por ejemplo, la introducción de nuevas funciones de SI o el número y la gravedad de las vulnerabilidades de SI que afectan a la versión actual). Los parches de software se deberían aplicar cuando puedan ayudar a eliminar o reducir las vulnerabilidades de SI (ver 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 monitorearse y controlarse para evitar cambios no autorizados ya que pueden introducir vulnerabilidades de SI. El software suministrado por el proveedor utilizado en los sistemas operativos debería mantenerse a un nivel respaldado 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 no compatible. El software de código abierto utilizado en los sistemas operativos debería mantenerse en la última versión apropiada del software. Con el tiempo, el código de código abierto puede dejar de mantenerse, pero sigue estando disponible en un repositorio de software de código abierto. La organización también debería considerar los riesgos de depender de software de código abierto no mantenido cuando se utiliza en sistemas operativos. 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. Es preciso monitorear las actividades del proveedor (ver 5.22). La organización debería definir y aplicar reglas estrictas sobre los tipos de software que los usuarios pueden instalar. El principio de privilegio mínimo debería aplicarse a la instalación de software en sistemas operativos. La organización debería identificar qué tipos de instalaciones de software están permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que solo es para uso personal y software cuyo origen con respecto a ser potencialmente malintencionado es desconocido o sospechoso). Estos privilegios deberían concederse en función de las funciones de los usuarios afectados.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

OTRA INFORMACIÓN	No hay más información.

8.20. SEGURIDAD DE LAS REDES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Detectivo #Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger #Detectar**	**#Seguridad_del_sistema_y_de_la red**	**#Protección**	**13.1.1**
CONTROL	Las redes y los dispositivos de red deberían estar protegidos, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.					
PROPÓSITO	Proteger la información de las redes y sus instalaciones de procesamiento de información de apoyo frente a riesgos a través de la red.					
ORIENTACIÓN	Deberían implementarse controles para garantizar la SI en las redes y para proteger los servicios conectados del acceso no autorizado. Especialmente, se deberían tomar en consideración los siguientes factores: a) determinar tipo y el nivel de clasificación de la información que admite la red; b) establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red; c) mantener documentación actualizada, incluidos diagramas de red y archivos de configuración de dispositivos (por ejemplo, routers, switches); d) separar la responsabilidad operativa de las redes de las operaciones de los sistemas de TIC cuando proceda (Ver 5.3); e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas, redes de terceros o redes inalámbricas y proteger los sistemas y aplicaciones conectados (ver 5.22, 8.24, 5.14 y 6.6). También pueden ser necesarios controles adicionales para mantener la disponibilidad de los servicios de red y de los computadores conectados a la red; f) registrar y supervisar las redes para permitir el registro y la detección de acciones que puedan afectar o sean relevantes para la SI (ver 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 aplican de forma coherente en toda la infraestructura de procesamiento de la información; h) autenticar los sistemas en la red; i) restringir y filtrar la conexión de los sistemas a la red (por ejemplo, mediante firewalls); j) detectar, restringir y autenticar la conexión de equipos y dispositivos a la red; k) reforzar de los dispositivos de red; l) separar los canales de administración de red de otro tráfico de red; m) aislar temporalmente subredes críticas (por ejemplo, con puentes levadizos) si la red está siendo atacada; n) desactivar de protocolos de red vulnerables. La organización debería asegurarse de que se aplican controles de seguridad adecuados al uso de redes virtualizadas. Las redes virtualizadas también abarcan 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 en redes físicas, especialmente para sistemas y aplicaciones que se implementan mediante informática distribuida.					
OTRA INFORMACIÓN	Información adicional sobre la seguridad de la red en la norma ISO/IEC 27033. Información sobre redes virtualizadas en la ISO/IEC 23167.					

8.21. SEGURIDAD DE LOS SERVICIOS DE RED

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_del_sistema_y_de_la_red**	**#Protección**	**13.1.3**
CONTROL	Deberían identificarse, implementarse y supervisarse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.					

PROPÓSITO	Garantizar la seguridad en el uso de los servicios de red.
ORIENTA-CIÓN	Las medidas de seguridad necesarias para determinados servicios, como las características de seguridad, los niveles de servicio y los requisitos de servicio, deberían ser identificadas e implementadas (por proveedores de servicios de red internos o externos). La organización debería asegurarse de que los proveedores de servicios de red implementan estas medidas. La capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura debería determinarse y supervisarse regularmente. El derecho a la auditoría debería acordarse entre la organización y el proveedor. La organización también debería tener en cuenta los certificados de terceros proporcionados por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas. Deberían formularse y aplicarse normas sobre la utilización de las redes y los servicios de red para abarcar: a) las redes y los servicios de red a los que se puede acceder; b) los requisitos de autenticación para acceder a diversos servicios de red; c) los procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red; d) la 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) la hora, ubicación y otros atributos del usuario en el momento del acceso; g) el monitoreo del uso de los servicios de red. Se deberían tener en cuenta las siguientes características de seguridad de los servicios de red: a) tecnología aplicada para la seguridad de los servicios de red, como la autenticación, el cifrado y los controles de conexión de red; b) parámetros técnicos necesarios para una conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión de red; c) almacenamiento en caché (por ejemplo, en una red de distribución 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.
OTRA IN-FORMACIÓN	Los servicios de red incluyen el suministro de conexiones, servicios de red privada y soluciones de seguridad de red administradas, como firewalls y sistemas de detección de intrusiones. Estos servicios pueden variar desde un ancho de banda simple no administrado hasta ofertas complejas de valor añadido. Más directrices sobre un marco para la gestión del acceso en la norma ISO/IEC 29146.

8.22. SEGREGACIÓN DE LAS REDES

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_del sistema_y_de_las redes**	**#Protección**	**13.1.3**
CONTROL	Los grupos de servicios de información, usuarios y sistemas de información deberían separarse en las redes de la organización.					
PROPÓSITO	Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de la organización.					
ORIENTA-CIÓN	La organización debería considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet). Los dominios se pueden elegir en función de los niveles de confianza, criticidad y sensibilidad (por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de bajo y alto riesgo), a lo largo de las unidades organizativas (por ejemplo, recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio de servidor que se conecta a varias unidades organizativas). La segregación se puede realizar al utilizar redes físicamente diferentes o al utilizar redes lógicas diferentes. El perímetro de cada dominio debería estar bien definido. Si se permite el acceso entre dominios de red, se debería controlar en el perímetro mediante una puerta de enlace (por					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	ejemplo, un firewall o un router de filtrado). Los criterios para la segregación de las redes en dominios y el acceso permitido a través de las puertas de enlace deberían basarse en una evaluación de los requisitos de seguridad de cada dominio. La evaluación debería realizarse de acuerdo con la política temática específica sobre control de acceso (ver 5.15), requisitos de acceso, valor y clasificación de la información procesada y tener en cuenta el costo relativo y el impacto en el desempeño de incorporar una tecnología de pasarela adecuada. Las redes inalámbricas requieren un tratamiento especial debido al perímetro de red mal definido. El ajuste de la cobertura de radio debería considerarse para la segregación de las redes inalámbricas. Para entornos sensibles, se debería considerar 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 puerta de enlace de acuerdo con los controles de red (ver 8.20) antes de conceder acceso a los sistemas internos. La red de acceso inalámbrico para invitados debería separarse de la del personal si el personal solo utiliza dispositivos de punto final de usuario controlados que cumplan las políticas específicas de la organización. El WiFi para invitados debería tener al menos las mismas restricciones que el WiFi para el personal, con el fin de desalentar el uso del WiFi para invitados por parte del personal.
OTRA INFORMACIÓN	Las redes a menudo se extienden más allá de los límites de la organización ya que se forman asociaciones empresariales que requieren la interconexión o el intercambio de servicios de procesamiento de la información y redes. Estas extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que utilizan la red, algunos de los cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.

8.23. FILTRADO WEB

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad del sistema y de las redes**	**#Protección**	**Nuevo**
CONTROL	El acceso a sitios web externos debería gestionarse para reducir la exposición a contenido malintencionado.					
PROPÓSITO	Para proteger los sistemas contra el peligro de malware y para evitar el acceso a recursos no autorizador de la web.					
ORIENTACIÓN	La organización debería reducir los riesgos de que su personal acceda a sitios web que contienen información ilegal o que se sabe que contienen virus o material de phishing. Una técnica para lograr esto funciona al bloquear la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware lo hacen automáticamente o pueden configurarse para hacerlo. La organización debería identificar los tipos de sitios web a los que el personal debería o no tener acceso. La organización debería considerar bloquear el acceso a los siguientes tipos de sitios web: a) sitios web que tengan una función de carga de información a menos que se permita por razones comerciales válidas; b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen contenido de malware o phishing); c) servidores de comando y control; d) sitio web malicioso adquirido de inteligencia contra amenazas (ver 5.7); e) sitios web que comparten contenido ilegal. Antes de implementar este control, la organización debería establecer reglas para un uso seguro y apropiado de recursos en línea, incluida cualquier restricción a sitios web indeseables o inadecuados y aplicaciones basadas en web. Las normas deberían mantenerse actualizadas. Se debería impartir capacitación al personal sobre el uso seguro y adecuado de los recursos en línea, incluido el acceso a la Web. La formación debería incluir las reglas de la organización, el punto de contacto para plantear problemas de seguridad y el proceso de excepción cuando se necesite acceder a recursos web restringidos por razones empresariales legítimas. También se debería impartir formación al personal para asegurarse de que no anulan ningún aviso del navegador que informe de que un sitio web no es seguro, pero que permite al usuario continuar.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

OTRA INFORMACIÓN	El filtrado web puede incluir una serie de técnicas, entre las que se incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a evitar que software malintencionado y otras actividades maliciosas ataquen la red y los sistemas de la organización.

8.24. USO DE CIFRADO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Configuración_segura**	**#Protección**	**10.1.1 10.1.2**
CONTROL	Se deberían definir e implementar reglas para el uso efectivo de la criptografía, incluida la administración de claves cifradas.					
PROPÓSITO	Garantizar el uso adecuado y efectivo del cifrado para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos de seguridad de la empresa y la información y tomando en consideración los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con el cifrado.					
ORIENTACIÓN	**General** Al utilizar el cifrado, se debería tener en cuenta lo siguiente: a) la directiva específica del tema sobre cifrado definida por la organización, incluidos los principios generales para la protección de la información. Es necesaria una política específica sobre el uso del cifrado para maximizar los beneficios y minimizar los riesgos de utilizar técnicas de cifrado y evitar un uso inapropiado o incorrecto; b) el nivel de protección requerido y la clasificación de la información y, en consecuencia, establecer el tipo, la fuerza y la calidad de los algoritmos cifrados necesarios; c) el uso del cifrado para la protección de la información contenida en dispositivos finales de usuario móvil o medios de almacenamiento y transmitida a través de redes a dichos dispositivos o medios de almacenamiento; d) el enfoque de la gestión de claves, incluidos los métodos para tratar la generación y protección de claves cifradas y la recuperación de información cifrada en caso de pérdida, compromiso o daño de claves; e) funciones y responsabilidades para: 1) la implementación de las reglas para el uso efectivo del cifrado; 2) la gestión de claves, incluida la generación de claves (ver 8.24); f) los estándares que se van a adoptar, así como los algoritmos cifrados, la fuerza del cifrado, las soluciones cifradas y las prácticas de uso aprobadas o requeridas para su uso en la organización; g) el impacto del uso de información cifrada en controles que dependen de la inspección de contenido (por ejemplo, detección de malware o filtrado de contenido). Al implementar las reglas de la organización para el uso efectivo del cifrado, se deberían tener en cuenta las regulaciones y restricciones nacionales que pueden aplicarse al uso de técnicas de cifrado en diferentes partes del mundo, así como los temas del flujo transfronterizo de información cifrada (ver 5.31). El contenido de los acuerdos de nivel de servicio o contratos con proveedores externos de servicios cifrados (por ejemplo, con una autoridad de certificación) debería abarcar cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta para la prestación de servicios (ver 5.22). **Gestión de claves** La gestión de claves adecuada requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves cifradas. Un sistema de gestión de claves debería basarse en un conjunto acordado de normas, procedimientos y métodos seguros para: a) generar claves para diferentes sistemas de cifrado y diferentes aplicaciones; b) emitir y obtener certificados de clave pública; c) distribuir claves a las entidades previstas, incluido cómo activar las claves cuando se reciben; d) almacenar las claves, incluida la forma en que los usuarios autorizados obtienen acceso a las claves; e) cambiar o actualizar claves, incluidas las reglas sobre cuándo cambiar claves y cómo se					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	hará esto; f) tratar con claves comprometidas; f) revocar las claves, incluido cómo retirar o desactivar claves (por ejemplo, cuando las claves se han puesto en peligro o cuando un usuario abandona una organización (en cuyo caso las claves también deberían archivarse)); g) recuperar claves que se pierden o están dañadas; h) realizar copias de seguridad o archivado de claves; i) destruir claves; j) registrar y auditar las actividades relacionadas con la gestión clave; k) establecer las fechas de activación y desactivación de las claves para que solo se puedan utilizar durante el período de tiempo de acuerdo con las reglas de la organización sobre la gestión de claves; l) gestionar solicitudes legales de acceso a claves cifradas (por ejemplo, se puede requerir que la información cifrada esté disponible en forma no cifrada como prueba en un caso judicial). Todas las claves cifradas deberían estar protegidas contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado, así como la divulgación. El equipo utilizado para generar, almacenar y archivar claves debería estar físicamente protegido. Además de la integridad, en muchos casos de uso, también debería considerarse la autenticidad de las claves públicas.
OTRA INFORMACIÓN	La autenticidad de las claves públicas se suele abordar mediante procesos de administración de claves públicas a través de autoridades de certificación y certificados de claves públicas, pero también es posible abordarla mediante tecnologías como la aplicación de procesos manuales para claves de número pequeño. El cifrado se puede utilizar para lograr diferentes PROPÓSITOS de SI, por ejemplo: a) confidencialidad: utilizar el cifrado de la información para proteger la información confidencial o crítica, almacenada o transmitida; b) integridad o autenticidad: utilizar firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información confidencial o crítica almacenada o transmitida. El uso de algoritmos para la comprobación de la integridad de los archivos; c) no rechazo: utilizar técnicas de cifrado para proporcionar pruebas de la ocurrencia o no ocurrencia de un evento o acción; d) autenticación: uso de técnicas de cifrado para autenticar usuarios y otras entidades del sistema que soliciten acceso o realicen transacciones con usuarios, entidades y recursos del sistema. Más información sobre la gestión de claves en la norma ISO/IEC 11770.

8.25. CICLO DE VIDA DE DESARROLLO SEGURO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_del_sistema_y_de_la_red**	**#Protección**	**14.2.1**
CONTROL	Deberían establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.					
PROPÓSITO	Garantizar que la SI se diseña e implementa dentro del ciclo de vida de desarrollo seguro del software y los sistemas.					
ORIENTACIÓN	El desarrollo seguro es un requisito para crear un servicio, una arquitectura, un software y un sistema seguros. Para lograr esto, se deberían tomar en consideración los siguientes factores: a) separación de entornos de desarrollo, pruebas y entornos de producción (ver 8.31); b) guía sobre la seguridad en el ciclo de vida de desarrollo de software: 1) seguridad en la metodología de desarrollo de software (ver 8.28 y 8.27); 2) directrices de codificación seguras para cada lenguaje de programación utilizado (ver 8.28); c) requisitos de seguridad en la fase de especificación y diseño (ver 5.8); d) puntos de control de seguridad en los proyectos (ver 5.8); e) pruebas de sistema y seguridad, como pruebas de regresión, análisis de código y					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	pruebas de penetración (ver 8.29); f) repositorios seguros para el código fuente y la configuración (ver 8.4 y 8.9); g) seguridad en el control de versiones (ver 8.32); h) conocimientos y formación necesarios sobre seguridad de las aplicaciones (ver el numeral 8.28); i) capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades (ver 8.28); j) requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (ver 5.32). Si se subcontrata el desarrollo, la organización debería obtener la garantía de que el proveedor cumple con las reglas de desarrollo seguro de la organización (ver 8.30).
OTRA INFORMACIÓN	El desarrollo también puede tener lugar dentro de aplicaciones, como aplicaciones de ofimática, secuencias de comandos, exploradores y bases de datos.

8.26. REQUISITOS DE SI

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_del_sistema_y_de_la_red**	**#Protección #Defensa**	**14.1.2 14.1.3**
CONTROL	Los requisitos de SI deberían ser identificados, especificados y aprobados al desarrollar o adquirir aplicaciones.					
PROPÓSITO	Garantizar que todos los requisitos de SI se identifican y se abordan al desarrollar o adquirir aplicaciones.					
ORIENTACIÓN	**General** Se deberían identificar y especificar los requisitos de seguridad de las aplicaciones. Estos requisitos se determinan generalmente a través de una evaluación de riesgos. Los requisitos deberían elaborarse con el apoyo de especialistas en SI. Los requisitos de seguridad de las aplicaciones pueden abarcar una amplia gama de temas, en función del propósito de la aplicación. Los requisitos de seguridad de las aplicaciones deberían incluir, según corresponda: a) nivel de confianza en la identidad de las entidades (por ejemplo, mediante autenticación (ver 5.17, 8.2 y 8.5)); b) tipo de información y el nivel de clasificación que debería procesar la solicitud; c) necesidad de segregación de acceso y nivel de acceso a los datos y funciones de la aplicación; d) resiliencia frente a ataques malintencionados o interrupciones no intencionadas (por ejemplo, protección contra desbordamiento de búfer o inyecciones de lenguaje de consulta estructurado (SQL)); e) requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción; f) necesidad de privacidad asociada a todas las partes implicadas; g) requisitos de protección de cualquier información confidencial; h) protección de datos mientras se procesan, en tránsito y en reposo; i) necesidad de cifrar de forma segura las comunicaciones entre todas las partes implicadas; j) controles de entrada, incluidas las comprobaciones de integridad y la validación de entrada; k) controles automatizados (por ejemplo, límites de aprobación o aprobaciones dobles); l) controles de salida, considerando también quién puede acceder a los resultados y su autorización; m) restricciones en torno al contenido de campos de texto libre ya que pueden conducir a un almacenamiento incontrolado de datos confidenciales (por ejemplo, datos personales); n) requisitos derivados del proceso de negocio, como el registro y la supervisión de las transacciones, los requisitos de no rechazo;					

	o) requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces para el registro y el monitoreo o sistemas de detección de fugas de datos); p) manejo de mensajes de error. **Servicios transaccionales** Adicionalmente, para las aplicaciones que ofrecen servicios transaccionales entre la organización y un socio, se debería considerar lo siguiente al identificar los requisitos de SI: a) el nivel de confianza que cada parte requiere en la identidad declarada de la otra; b) el nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para identificar la falta de integridad (por ejemplo, comprobación de redundancia cíclica, hashing, firmas digitales) c) los procesos de autorización asociados a quién puede aprobar el contenido de los documentos transaccionales clave, emitirlos o firmarlos; d) la confidencialidad, la integridad, la prueba de envío y de recepción de los documentos clave y el no repudio (por ejemplo, los contratos asociados a los procesos de licitación y de 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 la duración de la confidencialidad de una transacción; g) los seguros y otros requisitos contractuales. **Aplicaciones de pedidos y pagos electrónicos** Asimismo, en el caso de las aplicaciones que implican pedidos y pagos electrónicos, se debería tener en cuenta lo siguiente: a) los requisitos para mantener la confidencialidad e integridad de la información de los pedidos; b) el grado de verificación apropiado para comprobar la información de pago suministrada por un cliente; c) la pérdida o duplicación de la información de las transacciones; d) el almacenamiento de los datos de las transacciones fuera de cualquier entorno de acceso público (por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización y no conservada y expuesta en medios de almacenamiento electrónico directamente accesibles desde Internet); e) cuando se utilice una autoridad de confianza (por ejemplo, para la emisión y el mantenimiento de firmas certificados digitales), que la seguridad esté integrada e incorporada en todo el proceso de gestión de certificados o firmas de extremo a extremo. Varias de las consideraciones anteriores pueden abordarse mediante la aplicación de la criptografía (ver 8.24), tomando en consideración los requisitos legales (ver 5.31 a 5.36, especialmente 5.31 para la legislación sobre cifrado).
OTRA INFORMACIÓN	Las aplicaciones accesibles a través de las redes están sujetas a una serie de amenazas relacionadas con la red, como las actividades fraudulentas, los conflictos contractuales o la divulgación de información al público; la transmisión incompleta, el enrutamiento erróneo, la alteración no autorizada de mensajes, la duplicación o la repetición. Por lo tanto, es indispensable realizar evaluaciones de riesgo detalladas y determinar cuidadosamente los controles. Los controles necesarios suelen incluir métodos de cifrado para la autenticación y la seguridad de la transferencia de datos. Más información sobre la seguridad de las aplicaciones en la norma ISO/IEC 27034.

8.27. ARQUITECTURA DE SISTEMAS SEGUROS Y PRINCIPIOS DE INGENIERÍA SEGURA

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_del_sistema_y_de_la_red**	**#Protección**	**14.2.5**
CONTROL	Los principios para la ingeniería de sistemas seguros deberían establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.					

PROPÓSITO	Garantizar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida del desarrollo.
ORIENTACIÓN	Los principios de ingeniería de sistemas seguros se deberían establecer, documentar y aplicar a las actividades de ingeniería de los sistemas de información. La seguridad debería diseñarse en todas las capas de la arquitectura (negocio, datos, aplicaciones y tecnología). La nueva tecnología debería ser analizada para detectar los riesgos de seguridad y el diseño debería ser revisado contra los patrones de ataque conocidos. Los principios de ingeniería de seguridad proporcionan guía sobre las técnicas de autenticación de usuarios, el control de sesiones seguras y la validación y saneamiento de datos. Los principios de ingeniería de sistemas seguros deberían incluir el análisis de: a) la variedad de controles de seguridad necesarios para proteger la información y los sistemas contra las amenazas identificadas; b) las capacidades de los controles de seguridad para prevenir, detectar o responder a eventos de seguridad; c) los controles de seguridad específicos que requieren determinados procesos empresariales (por ejemplo, el cifrado de información sensible, la comprobación de la integridad de la firma digital de la información); d) dónde y cómo deberían aplicarse los controles de seguridad (por ejemplo, mediante la integración con una arquitectura de seguridad y la infraestructura técnica); e) cómo funcionan los controles de seguridad individuales (manuales y automáticos) para producir un conjunto integrado de controles. Los principios de ingeniería de seguridad deberían tener en cuenta: a) la necesidad de integrarse con una arquitectura de seguridad; b) infraestructura técnica de seguridad (por ejemplo, infraestructura de clave pública (PKI), gestión de la identidad y el acceso (IAM), prevención de la fuga de datos y gestión dinámica del acceso); c) capacidad de la organización para desarrollar y apoyar la tecnología elegida; d) el costo, el tiempo y la complejidad de cumplir con los requisitos de seguridad; e) las buenas prácticas actuales. La ingeniería de sistemas seguros debería incluir: a) el uso de principios de arquitectura de seguridad, como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación por defecto", "falla segura", "desconfianza en la entrada de aplicaciones externas", "seguridad en el despliegue", "asumir el incumplimiento", "mínimo privilegio", "usabilidad y manejabilidad" y "mínima funcionalidad"; b) una revisión del diseño centrada en la seguridad para ayudar a identificar las vulnerabilidades de la SI, garantizar que se especifican los controles de seguridad y cumplir con los requisitos de seguridad; c) la documentación y el reconocimiento formal de los controles de seguridad que no cumplen plenamente los requisitos (por ejemplo, debido a requisitos de seguridad imperativos); d) fortalecimiento de los sistemas. La organización debería considerar los principios de "confianza cero", tales como a) asumir que los sistemas de información de la organización ya han sido vulnerados y, por tanto, no depender únicamente de la seguridad del perímetro de la red; b) emplear un enfoque de "nunca confiar y siempre verificar" para el acceso a los sistemas de información; c) garantizar que las solicitudes a los sistemas de información estén cifradas de principio a fin; d) verificar cada solicitud a un sistema de información como si se originara en una red abierta y externa, incluso si estas solicitudes se originan dentro de la organización (es decir, no confiar automáticamente en nada dentro o fuera de sus perímetros); e) utilizar técnicas de control de acceso dinámico y de "mínimo privilegio" (ver los numerales 5.15, 5.18 y 8.2). Esto incluye la autenticación y autorización de las solicitudes de información o a los sistemas en función de la información contextual, como la información de autenticación (ver 5.17), las identidades de los usuarios (ver el numeral 5.16), los datos sobre el dispositivo del usuario y la clasificación de los datos (ver 5.12); f) autenticar siempre a los solicitantes y validar siempre las solicitudes de autorización a los sistemas de información sobre la base de información que incluya la información de

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	autenticación (ver 5.17) y las identidades de los usuarios (ver el numeral 5.16), los datos sobre el dispositivo final del usuario y la clasificación de los datos (ver 5.12), por ejemplo, aplicando una autenticación fuerte (por ejemplo, multifactorial, ver 8.5). Se deberían aplicar los principios de ingeniería de sistemas seguros establecidos, cuando sea aplicable, al desarrollo externo de sistemas de información a través de los contratos y otros acuerdos vinculantes entre la organización y el proveedor al que la organización subcontrata. La organización debería asegurarse de que las prácticas de ingeniería de sistemas seguros de los proveedores se ajusten a las necesidades de la organización. Los principios de ingeniería de sistemas seguros y los procedimientos de ingeniería establecidos deberían revisarse periódicamente para garantizar que contribuyen efectivamente a mejorar los estándares de seguridad dentro del proceso de ingeniería. También deberían revisarse periódicamente para garantizar que se mantienen actualizados en lo que respecta a la lucha contra cualquier nueva amenaza potencial y para que sigan siendo aplicables a los avances en las tecnologías y soluciones que se aplican.
OTRA INFORMACIÓN	Los principios de la ingeniería de sistemas seguros pueden aplicarse al diseño o la configuración de una serie de técnicas, como: - tolerancia a fallas y otras técnicas de resiliencia; - segregación (por ejemplo, mediante la virtualización o la contenerización) - resistencia a la manipulación. Las técnicas de virtualización segura pueden utilizarse para evitar la interferencia entre las aplicaciones que se ejecutan en el mismo dispositivo físico. Si una instancia virtual de una aplicación se ve comprometida por un atacante, solo esa instancia se ve afectada. El ataque no tiene efecto sobre ninguna otra aplicación o datos. Las técnicas de resistencia a la manipulación pueden utilizarse para detectar la manipulación de contenedores de información ya sean físicos (por ejemplo, una alarma antirrobo) o lógicos (por ejemplo, un archivo de datos). Una característica de estas técnicas es que queda constancia del intento de manipulación del contenedor. Además, el control puede impedir que se extraigan con éxito los datos mediante su destrucción (por ejemplo, se puede borrar la memoria del dispositivo).

8.28. CODIFICACION SEGURA

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_del_sistema_y_de_la_red**	**#Protección**	**Nuevo**
CONTROL	Los principios de codificación segura se deberían aplicar al desarrollo del software.					
PROPÓSITO	Garantizar que el software se codifica de forma segura, lo que reduce el número de posibles vulnerabilidades de SI en el software.					
ORIENTACIÓN	**General** La organización debería establecer procesos en toda la organización para proporcionar un buen gobierno para la codificación segura. Debería establecerse y aplicarse una base mínima de seguridad. Además, estos procesos y el gobierno deberían ampliarse para cubrir los componentes de software de terceros y el software de código abierto. La organización debería supervisar las amenazas del mundo real y los consejos e información actualizados sobre las vulnerabilidades del software para guiar los principios de codificación segura de la organización a través de la mejora y el aprendizaje continuos. Esto puede ayudar a garantizar la aplicación de prácticas eficaces de codificación segura para combatir el cambiante panorama de las amenazas. **Planificación y antes de la codificación** Los principios de codificación segura deberían utilizarse tanto en los nuevos desarrollos como en los escenarios de reutilización. Estos principios deberían aplicarse a las actividades de desarrollo tanto dentro de la organización como para los productos y servicios suministrados por la organización a otros. La planificación y los requisitos previos a la codificación deberían incluir:					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	a) expectativas específicas de la organización y los principios aprobados para la codificación segura que se utilizarán tanto para los desarrollos de código internos como para los subcontratados; b) prácticas de codificación comunes e históricas y defectos que conducen a vulnerabilidades de SI; c) configuración de las herramientas de desarrollo, como los entornos de desarrollo integrados (IDE), para ayudar a imponer la creación de código seguro; d) seguimiento las directrices emitidas por los proveedores de herramientas de desarrollo y entornos de ejecución, según proceda; e) mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores); f) calificación de los desarrolladores en la escritura de código seguro; g) diseño y arquitectura seguros, incluida la modelización de amenazas; h) normas de codificación segura y, en su caso obligatoriedad de su uso; i) uso de entornos controlados para el desarrollo durante la codificación. Las consideraciones durante la codificación deberían incluir: a) prácticas de codificación segura específicas de los lenguajes y técnicas de programación que se utilicen; b) uso de técnicas de programación seguras, como la programación por parejas, la refactorización, la revisión por pares, las iteraciones de seguridad y el desarrollo basado en pruebas; c) uso técnicas de programación estructurada; d) documentación del código y eliminar los defectos de programación, que pueden permitir la explotación de las vulnerabilidades de la SI; e) prohibición del uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, muestras de código no aprobadas y servicios web no autenticados). Las pruebas deberían realizarse durante y después del desarrollo (ver 8.29). Los procesos de pruebas estáticas de seguridad de las aplicaciones (SAST) pueden identificar vulnerabilidades de seguridad en el software. Antes de que el software se ponga en funcionamiento, debería evaluarse lo siguiente: a) la superficie de ataque y el principio de mínimo privilegio; b) la realización de un análisis de los errores de programación más comunes y la documentación de que se han mitigado. **Revisión y mantenimiento** Una vez que el código se ha hecho operativo: a) las actualizaciones deberían ser empaquetadas y desplegadas de forma segura; b) el tratamiento de las vulnerabilidades de SI notificadas (ver 8.8); c) los errores y las sospechas de ataques deberían anotarse y los registros deberían revisarse periódicamente para realizar los ajustes necesarios en el código; d) el código fuente debería estar protegido contra el acceso no autorizado y la manipulación (por ejemplo, mediante el uso de herramientas de gestión de la configuración, que suelen ofrecer funciones como el control de acceso y el control de versiones). Si se utilizan herramientas y bibliotecas externas, la organización debería considerar: a) asegurar que las bibliotecas externas se gestionan (por ejemplo, mediante el mantenimiento de un inventario de las bibliotecas utilizadas y sus versiones) y que se actualizan regularmente con los ciclos de lanzamiento; b) seleccionar, autorizar y reutilizar componentes bien examinados, en particular los componentes de autenticación y cifrado; c) asegurar el licenciamiento, la seguridad y el historial de los componentes externos; d) garantizar que el software es mantenible, tiene un seguimiento y procede de fuentes acreditadas y de confianza; e) asegurar la disponibilidad a largo plazo de los recursos y artefactos de desarrollo. Cuando sea necesario modificar un paquete de software, deberían tenerse en cuenta los siguientes puntos: a) el riesgo de que los controles incorporados y los procesos de integridad se vean comprometidos; b) la posibilidad de obtener el consentimiento del proveedor; c) la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones estándar del programa; d) el impacto si la organización se hace responsable del futuro mantenimiento del software

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	como resultado de los cambios; e) la compatibilidad con otros programas informáticos en uso.
OTRA INFORMACIÓN	Un principio rector es garantizar que el código pertinente para la seguridad se invoque cuando sea necesario y sea resistente a las manipulaciones. Los programas instalados a partir de código binario compilado también tienen estas propiedades, pero solo para los datos contenidos en la aplicación. En el caso de los lenguajes interpretados, el concepto solamente funciona cuando el código se ejecuta en un servidor inaccesible para los usuarios y procesos que lo utilizan y que sus datos se guardan en una base de datos igualmente protegida. Por ejemplo, el código interpretado puede ejecutarse en un servicio en la nube donde el acceso al propio código requiere privilegios de administrador. Este 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 un acceso remoto directo al servidor, en principio también puede hacerlo un atacante. Los servidores web deberían estar configurados para impedir la navegación por los directorios en estos casos. La mejor manera de diseñar el código de las aplicaciones es partiendo de la base de que siempre es susceptible de ser atacado, por error o por acción maliciosa. Además, las aplicaciones críticas pueden diseñarse para ser tolerantes a las fallas internos. Por ejemplo, la salida de un algoritmo complejo puede comprobarse para asegurar que se encuentra dentro de los límites de seguridad antes de que los datos se utilicen en una aplicación como una aplicación crítica de seguridad o financiera. El código que realiza las comprobaciones de los límites es sencillo y, por tanto, mucho más fácil de demostrar su corrección. Algunas aplicaciones web son susceptibles de sufrir una serie de vulnerabilidades introducidas por un diseño y una codificación deficientes, como la inyección en la base de datos y los ataques de scripting entre sitios. En estos ataques, las peticiones pueden ser manipuladas para abusar de la funcionalidad del servidor web. Más información sobre la evaluación de la seguridad de las TIC en la norma ISO/IEC 15408.

8.29. PRUEBAS DE SEGURIDAD Y DE ACEPTACION EN EL DESARROLLO

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_de_la_información #Seguridad_del_sistema_y_de_la_red**	**#Protección**	**14.2.8 14.2.9**
CONTROL	Los procesos de pruebas de seguridad deberían definirse e implementarse en el ciclo de vida del desarrollo.					
PROPÓSITO	Validar si se cumplen los requisitos de SI cuando las aplicaciones o el código se despliegan en el entorno de producción.					
ORIENTACIÓN	Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deberían probarse y verificarse a fondo durante los procesos de desarrollo. Las pruebas de seguridad deberían ser una parte integral de las pruebas de los sistemas o componentes. Las pruebas de seguridad deberían realizarse en función de 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 (ver 8.5), restricción de acceso (ver 8.3) y uso de cifrado (ver 8.24)); b) codificación segura (ver 8.28); c) configuraciones seguras (ver 8.9, 8.20 y 8.22), incluidas las de los sistemas operativos, los cortafuegos y otros componentes de seguridad. Los planes de pruebas deberían determinarse mediante 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 introducido. El plan de pruebas debería incluir: a) un calendario detallado de actividades y pruebas; b) las entradas y salidas previstas en una serie de condiciones;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	c) criterios para evaluar los resultados; d) decisión sobre las acciones posteriores que sean necesarias. La organización puede aprovechar las herramientas automatizadas, por ejemplo, las herramientas de análisis de código o los escáneres de vulnerabilidad y debería verificar la corrección de los defectos relacionados con la seguridad. En el caso de los desarrollos internos, estas pruebas deberían ser realizadas inicialmente por el equipo de desarrollo. A continuación, deberían realizarse pruebas de aceptación independientes para garantizar que el sistema funciona como se espera y solo como se espera (ver 5.8). Debería tenerse en cuenta la realización de: a) actividades de revisión del código como elemento relevante para la comprobación de las fallas de seguridad, incluidas las entradas y condiciones no previstas; b) escaneos de vulnerabilidad para identificar configuraciones inseguras y vulnerabilidades del sistema; c) pruebas de penetración para identificar el código y el diseño inseguros. En el caso de los componentes de desarrollo y compra subcontratados, debería seguirse un proceso de adquisición. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados (ver 5.20). Los productos y servicios deberían ser evaluados según estos criterios antes de su adquisición. Las pruebas deberían realizarse en un entorno de pruebas que se ajuste lo más posible al entorno de producción objetivo para garantizar que el sistema no introduce vulnerabilidades en el entorno de la organización y que las pruebas son fiables (ver 8.31).
OTRA INFORMACIÓN	Se pueden establecer múltiples entornos de prueba, que se pueden utilizar para diferentes tipos de pruebas (por ejemplo, pruebas funcionales y de rendimiento). Estos diferentes entornos pueden ser virtuales, con configuraciones individuales para simular una variedad de entornos operativos. También hay que tener en cuenta las pruebas y monitoreo de los entornos de prueba, las herramientas y las tecnologías para garantizar la eficacia de las pruebas. Las mismas consideraciones se aplican a la supervisión de los sistemas de control desplegados en los entornos de desarrollo, prueba y producción. Es necesario tener criterio, guiado por la sensibilidad de los sistemas y los datos, para determinar cuántas capas de metapruebas son útiles.

8.30. DESARROLLO TERCERIZADO

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo #Detectivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Identificar #Proteger #Detectar**	**#Seguridad_de_las_aplicaciones #Seguridad_del_sistema_y_de_la_red #Seguridad_de_las_relaciones_con_los proveedores**	**#Gobierno_y_ecosistema #Protección**	**14.2.7**
CONTROL	La organización debería controlar, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas tercerizados.					
PROPÓSITO	Garantizar la aplicación de las medidas de SI requeridas por la organización en el desarrollo de sistemas tercerizados.					
ORIENTACIÓN	En los casos en que el desarrollo del sistema se subcontrata, la organización debería comunicar y acordar los requisitos y expectativas y monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con estas expectativas. Los siguientes puntos deberían considerarse en toda la cadena de suministro externa de la organización: a) acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado (ver 5.32); b) requisitos contractuales para las prácticas de diseño, codificación y pruebas seguras (ver 8.25 al 8.29); c) suministro del modelo de amenaza a considerar por desarrolladores externos; d) pruebas de aceptación de la calidad y exactitud de los resultados (ver 8.29); e) suministro de pruebas de que se han establecido niveles mínimos aceptables de					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	capacidades de seguridad y privacidad (por ejemplo, informes de garantía); f) pruebas de que se han realizado pruebas suficientes para evitar la presencia de contenidos maliciosos (tanto intencionados como no intencionados) en el momento de la entrega; g) pruebas de que se han realizado pruebas suficientes para evitar la presencia de vulnerabilidades conocidas; h) acuerdos de custodia del código fuente del software (por ejemplo, si el proveedor quiebra o desaparece); i) derecho contractual a auditar los procesos y controles de desarrollo; j) requisitos de seguridad para el entorno de desarrollo (ver 8.31); k) tomando en consideración la legislación aplicable (por ejemplo, sobre protección de datos personales).
OTRA INFORMACIÓN	Más información sobre las relaciones con los proveedores en la norma ISO/IEC 27036.

8.31. SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_de_las_relaciones_con_los proveedores**	**#Protección**	**12.1.4 14.2.6**
CONTROL	Los entornos de desarrollo, prueba y producción deberían estar separados y protegidos.					
PROPÓSITO	Proteger el entorno de producción y los datos del peligro que suponen las actividades de desarrollo y prueba.					
ORIENTACIÓN	Debería identificarse y aplicarse el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción. Se deberían tomar en consideración los siguientes factores: a) separar adecuadamente los sistemas de desarrollo y producción y hacerlos funcionar en dominios diferentes (por ejemplo, en entornos virtuales o físicos separados); b) definir, documentar y aplicar normas y autorizaciones para el despliegue de software desde el estado de desarrollo al de producción; c) probar los cambios en los sistemas y aplicaciones de producción en un entorno de prueba o de ensayo antes de aplicarlos a los sistemas de producción (ver 8.29); d) no realizar pruebas en entornos de producción, salvo en circunstancias definidas y aprobadas; e) impedir el acceso desde los sistemas de producción a los compiladores, editores y otras herramientas de desarrollo o programas de utilidad, cuando no sean necesario; f) mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error; g) no copiar información sensible en los entornos de los sistemas de desarrollo y de prueba, a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y de prueba. En todos los casos, los entornos de desarrollo y prueba deberían estar protegidos tomando en consideración: a) la aplicación de parches y la actualización de todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y bibliotecas); b) configuración segura de los sistemas y programas informáticos; c) control de acceso a los entornos; d) monitoreo de los cambios en el ambiente y en el código almacenado en el mismo; e) supervisión segura de los entornos; f) realización de copias de seguridad de los entornos. Una sola persona no debería tener la capacidad de realizar cambios tanto en el desarrollo como en la producción sin revisión y aprobación previas. Esto puede lograrse, por ejemplo, mediante la separación de los derechos de acceso o mediante reglas supervisadas. En situaciones excepcionales, deberían aplicarse medidas adicionales, como el registro detallado					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	y la supervisión en tiempo real, para detectar los cambios no autorizados y actuar en consecuencia.
OTRA INFORMACIÓN	Sin las medidas y procedimientos adecuados, los desarrolladores y probadores que tienen acceso a los sistemas de producción pueden introducir riesgos significativos (por ejemplo, modificación no deseada de los archivos o del entorno del sistema, fallas del sistema, ejecución de código no autorizado y no probado en los sistemas de producción, divulgación de datos confidenciales, problemas de integridad y disponibilidad de los datos). Es necesario mantener un entorno conocido y estable en el que se puedan realizar pruebas significativas y evitar el acceso inadecuado de los desarrolladores al entorno de producción. Las medidas y los procedimientos incluyen el diseño cuidadoso de las funciones junto con la aplicación de los requisitos de separación de funciones y el establecimiento de procesos de supervisión adecuados. El personal de desarrollo y pruebas también supone una amenaza para la confidencialidad de la información de producción. Las actividades de desarrollo y prueba pueden provocar cambios no deseados en el software o la información si comparten el mismo entorno informático. Por lo tanto, es conveniente separar los entornos de desarrollo, pruebas y producción para reducir el riesgo de cambios accidentales o de acceso no autorizado al software de producción y a los datos de la empresa (ver 8.33 para la protección de la información de pruebas). En algunos casos, la distinción entre los entornos de desarrollo, prueba y producción puede ser deliberadamente borrosa y las pruebas se pueden llevar a cabo en un entorno de desarrollo o a través de despliegues controlados a usuarios o servidores en vivo (por ejemplo, una pequeña población de usuarios piloto). En algunos casos, las pruebas del producto se pueden realizar mediante el uso en vivo del producto dentro de la organización. Además, para reducir el tiempo de inactividad de los despliegues en vivo, se puede dar soporte a dos entornos de producción idénticos en los que solo uno esté en vivo en un momento dado. Se requieren procesos de apoyo para el uso de datos de producción en entornos de desarrollo y pruebas (ver 8.33). Las organizaciones también pueden tomar en consideración las orientaciones proporcionadas en esta sección para los entornos de formación cuando realicen la formación de los usuarios finales.

8.32. GESTIÓN DE CAMBIOS

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_de_las_aplicaciones #Seguridad_del_sistem_y_de_la_red**	**#Protección**	**12.1.2 14.2.2 14.2.3 14.2.4**
CONTROL	Los cambios en las instalaciones de procesamiento de la información y en los sistemas de información deberían estar sujetos a procedimientos de gestión del cambio.					
PROPÓSITO	Para preservar la SI al ejecutar los cambios.					
ORIENTACIÓN	La introducción de nuevos sistemas y de cambios importantes en los sistemas existentes debería seguir unas normas acordadas y un proceso formal de documentación, especificación, pruebas, control de calidad y aplicación gestionada. Deberían establecerse responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios. Los procedimientos de control de cambios deberían documentarse y aplicarse para garantizar la confidencialidad, la integridad y la disponibilidad de la información en las instalaciones de procesamiento de la información y en los sistemas de información, para todo el ciclo de vida de desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores. Siempre que sea posible, los procedimientos de control de cambios para la infraestructura y el software de las TIC deberían estar integrados. Los procedimientos de control de cambios deberían incluir: a) planificar y evaluar el impacto potencial de los cambios tomando en consideración todas las dependencias;					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

	b) autorizar los cambios; c) comunicar los cambios a las partes interesadas pertinentes; d) realizar pruebas internas y pruebas de aceptación para los cambios (ver 8.29); e) aplicar los cambios, incluidos los planes de despliegue; f) consideraciones de emergencia y contingencia, incluidos los procedimientos de repliegue (rollback); g) mantener registros de los cambios que incluyan todo lo anterior; h) garantizar que la documentación de funcionamiento (ver 5.37) y los procedimientos de los usuarios se modifiquen según sea necesario para que sigan siendo adecuados; i) garantizar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación (ver 5.30) se modifiquen según sea necesario para seguir siendo adecuados.
OTRA INFORMACIÓN	El control inadecuado de los cambios en las instalaciones de procesamiento de la información y en los sistemas de información es una causa común de fallas en el sistema o en la seguridad. Los cambios en el entorno de producción, especialmente cuando se transfiere el software del entorno de desarrollo al operativo, pueden repercutir en la integridad y disponibilidad de las aplicaciones. Los cambios en el software pueden afectar al entorno de producción y viceversa. Las buenas prácticas incluyen la comprobación de los componentes de las TIC en un entorno separado de los entornos de producción y desarrollo (ver 8.31). Esto proporciona un medio para tener control sobre el nuevo software y permite una protección adicional de la información operativa que se utiliza para fines de prueba. Esto debería incluir parches, paquetes de servicio y otras actualizaciones. El entorno de producción incluye los sistemas operativos, las bases de datos y las plataformas de middleware. El control debería aplicarse a los cambios de aplicaciones e infraestructuras.

8.33. INFORMACIÓN PARA LAS PRUEBAS

ATRIBUTOS	**Tipo de Control**	**Propiedades de la SI**	**Conceptos de Ciberseguridad**	**Capacidades operativas**	**Dominios de Seguridad**	**CONTROLES ISO/IEC 27002:2013**
	#Preventivo	**#Confidencialidad #Integridad**	**#Proteger**	**#Protección_de_la_información**	**#Protección**	**14.3.1**
CONTROL	La información para las pruebas debería seleccionarse, protegerse y gestionarse adecuadamente.					
PROPÓSITO	Garantizar la pertinencia de las pruebas y la protección de la información operativa utilizada para las mismas.					
ORIENTACIÓN	La información para las pruebas debería seleccionarse para garantizar la fiabilidad de los resultados de las pruebas y la confidencialidad de la información operativa pertinente. La información sensible (incluida la información de identificación personal) no debería copiarse en los entornos de desarrollo y pruebas (ver 8.31). Las siguientes directrices deberían aplicarse para proteger las copias de la información operativa, cuando se utilicen con fines de prueba, tanto si el entorno de prueba se construye internamente como en un servicio en la nube: a) aplicar a los entornos de prueba los mismos procedimientos de control de acceso que se aplican a los entornos operativos; b) tener una autorización independiente cada vez que se copie información operativa en un entorno de pruebas; c) registrar la copia y el uso de la información operativa para proporcionar un registro de auditoría; d) proteger la información sensible mediante su eliminación o enmascaramiento (ver 8.11) si se utiliza para las pruebas; e) eliminar adecuadamente (ver 8.10) la información operativa de un entorno de prueba inmediatamente después de que se haya completado la prueba para evitar el uso no autorizado de la información de prueba. La información de las pruebas debería almacenarse de forma segura (para evitar su manipulación, que puede dar lugar a resultados no válidos) y utilizarse únicamente con fines de prueba.					
OTRA IN-	Las pruebas de sistemas y de aceptación pueden requerir volúmenes considerables de					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

FORMACIÓN	información de prueba que se acerquen lo más posible a la información operativa.

8.34. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE AUDITORÍA

	Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de Seguridad	CONTROLES ISO/IEC 27002:2013
ATRIBUTOS	**#Preventivo**	**#Confidencialidad #Integridad #Disponibilidad**	**#Proteger**	**#Seguridad_del_sistema_y_de_la_red #Protección_de_la_información**	**#Gobierno_y_ecosistema #Protección**	**12.7.1**
CONTROL	Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos deberían planificarse y acordarse entre el encargado de las pruebas y la dirección correspondiente.					
PROPÓSITO	Minimizar el impacto de las auditorías y otras actividades de garantía en los sistemas operativos y los procesos empresariales.					
ORIENTACIÓN	Deberían observarse las siguientes directrices: a) acordar las solicitudes de auditoría para el acceso a los sistemas y datos con la dirección correspondiente; b) acordar y controlar el alcance de las pruebas técnicas de auditoría; c) limitar las pruebas de auditoría al acceso de solo lectura a los programas y datos. Si no se dispone de acceso de solo lectura para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor; d) si se concede el acceso, establecer y verificar los requisitos de seguridad (por ejemplo, antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (por ejemplo, computadores portátiles o tabletas) antes de permitir el acceso; e) permitir solo el acceso a copias aisladas de los archivos del sistema que no sean de solo lectura y borrarlas una vez finalizada la auditoría o darles la protección adecuada si existe la obligación de conservar dichos archivos en virtud de los requisitos de la documentación de auditoría; 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 a la disponibilidad del sistema fuera del horario laboral; h) supervisar y registrar todos los accesos con fines de auditoría y prueba.					
OTRA INFORMACIÓN	Las pruebas de auditoría y otras actividades de aseguramiento también pueden tener lugar en los sistemas de desarrollo y de prueba, donde dichas pruebas pueden afectar, por ejemplo, a la integridad del código o llevar a la divulgación de cualquier información sensible que se encuentre en dichos entornos.					

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ANEXO A: UTILIZACIÓN DE ATRIBUTOS

A.1 GENERAL

Los atributos se pueden usar para crear diferentes vistas de los controles. Los cinco ejemplos de atributos son (ver 4.2):

a) Tipos de control (#Preventivo, #Detectivo, #Correctivo)

b) Propiedades de SI (#Confidencialidad, #Integridad, #Disponibilidad)

c) Conceptos de ciberseguridad (#Identificar, #Proteger, #Detectar, #Responder, #Recuperar)

d) Capacidades operativas (#Gobierno, #Gestión_de_activos, #Protección_de_la_información, #Seguridad_de_los_recursos_humanos, #Seguridad_física, #Seguridad_de_sistema_y_la_red, #Seguridad_de_las_aplicaciones, #Configuración_segura, #Gestión_de_identidades_y_accesos, Gestión_de_amenazas_y_vulnerabilidades, #Continuidad, #Seguridad_de_las_relaciones_con_los_proveedores, #Legal_y_cumplimiento, #Gestión_de_eventos_de_SI, #Aseguramiento_de_la_SI)

e) Dominios de seguridad (#Gobierno_y_Ecosistema, #Protección, #Defensa, #Resiliencia).

ANEXO B CORRESPONDENCIA DE LA ISO/IEC 27002:2022 CON LA ISO/IEC 27002:2013

El propósito de este anexo es proporcionar compatibilidad con la norma ISO/IEC 27002:2013 para las organizaciones que actualmente están al utilizar esa norma y ahora desean hacer la transición a esta edición.

En la última columna de las filas que describen los ATRIBUTOS de cada control se especifica la correspondencia con la ISO/IEC 27002:2013.

La tabla siguiente proporciona la correspondencia de los controles especificados en la ISO/IEC 27002:2013 con los de esta norma.

ISO/IEC 27002:2013	ISO/IEC 27002:2022	Nombre de control de acuerdo con la norma ISO/IEC 27002:2013
5		**Políticas de SI**
5.1		Dirección de la gestión de la SI
5.1.1	5.1	Políticas de SI
5.1.2	5.1	Revisión de las políticas de SI
6		**Organización de la SI**
6.1		Organización interna
6.1.1	5.2	Funciones y responsabilidades en materia de SI
6.1.2	5.3	Segregación de funciones
6.1.3	5.5	Contacto con las autoridades
6.1.4	5.6	Contacto con grupos de interés especiales
6.1.5	5.8	SI en la gestión de proyectos
6.2		Dispositivos móviles y teletrabajo
6.2.1	8.1	Política de dispositivos móviles
6.2.2	6.7	Teletrabajo
7		**Seguridad de los recursos humanos**
7.1		Precontratación
7.1.1	6.1	Selección
7.1.2	6.2	Condiciones del empleo
7.2		Durante el empleo
7.2.1	5.4	Responsabilidades de gestión

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ISO/IEC 27002:2013	ISO/IEC 27002:2022	Nombre de control de acuerdo con la norma ISO/IEC 27002:2013
7.2.2	6.3	Sensibilización, educación y formación en materia de SI
7.2.3	6.4	Proceso disciplinario
7.3		Terminación y cambio de empleo
7.3.1	6.5	Cese o cambio de responsabilidades laborales
8		**Gestión de activos**
8.1		Responsabilidad de los activos
8.1.1	5.9	Inventario de activos
8.1.2	5.9	Propiedad de los activos
8.1.3	5.10	Uso aceptable de los activos
8.1.4	5.11	Devolución de activos
8.2		Clasificación de 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	Manejo de activos
8.3		Manejo de los medios de almacenamiento
8.3.1	7.10	Gestión de medios extraíbles
8.3.2	7.10	Eliminación de medios de almacenamiento
8.3.3	7.10	Transferencia de medios físicos
9		**Control de acceso**
9.1		Requisitos comerciales del control de acceso
9.1.1	5.15	Política de control de acceso
9.1.2	5.15	Acceso a redes y servicios de red
9.2		Gestión del acceso de los usuarios
9.2.1	5.16	Registro y baja de usuarios
9.2.2	5.18	Aprovisionamiento del acceso de los usuarios
9.2.3	8.2	Gestión de los derechos de acceso privilegiados
9.2.4	5.17	Gestión de la información secreta de autentificación de los usuarios
9.2.5	5.18	Revisión de los derechos de acceso del usuario
9.2.6	5.18	Eliminación o ajuste de los derechos de acceso
9.3		Responsabilidades del usuario
9.3.1	5.17	Uso de información secreta de autenticación
9.4		Control de acceso al sistema y a las 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 programas de utilidad privilegiados
9.4.5	8.4	Control de acceso al código fuente del programa
10		**Cifrado**
10.1		Controles de cifrados
10.1.1	8.24	Política de uso de controles cifrados
10.1.2	8.24	Gestión de claves
11		**Seguridad física y medioambiental**
11.1		Zonas seguras
11.1.1	7.1	Perímetros de seguridad física
11.1.2	7.2	Controles físicos de entrada
11.1.3	7.3	Protección de oficinas, salas e instalaciones
11.1.4	7.5	Protección contra las amenazas externas y medioambientales
11.1.5	7.6	Trabajo en zonas seguras
11.1.6	7.2	Zonas de entrega y carga
11.2		Equipo
11.2.1	7.8	Ubicación y protección de los equipos
11.2.2	7.11	Servicios públicos de respaldo
11.2.3	7.12	Seguridad del cableado
11.2.4	7.13	Mantenimiento del equipo
11.2.5	7.10	Retiro de activos
11.2.6	7.9	Seguridad de equipos y activos fuera de las instalaciones
11.2.7	7.14	Eliminación segura o reutilización de los equipos
11.2.8	8.1	Equipo de usuario desatendido
11.2.9	7.7	Política de escritorio limpio y pantalla limpia
12		**Seguridad de las operaciones**

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ISO/IEC 27002:2013	ISO/IEC 27002:2022	Nombre de control de acuerdo con la norma ISO/IEC 27002:2013
12.1		Procedimientos operacionales y responsabilidades
12.1.1	5.37	Procedimientos operativos documentados
12.1.2	8.32	Gestión del cambio
12.1.3	8.6	Gestión de capacidad
12.1.4	8.31	Separación de los entornos de desarrollo, prueba y operación
12.2		Protección contra el malware
12.2.1	8.7	Controles contra malware
12.3		Copia de seguridad
12.3.1	8.13	Copia de SI
12.4		Registro y monitoreo
12.4.1	8.15	Registro de evento
12.4.2	8.15	Protección de la información de registro
12.4.3	8.15	Registros del administrador y del operador
12.4.4	8.17	Sincronización del reloj
12.5		Control del software operativo
12.5.1	8.19	Instalación de software en sistemas operativos
12.6		Gestión de la vulnerabilidad técnica
12.6.1	8.8	Gestión de las vulnerabilidades técnicas
12.6.2	8.19	Restricciones a la instalación de software
12.7		Consideraciones sobre la auditoría de los sistemas de información
12.7.1	8.34	Controles de auditoría de los sistemas de información
13		**Seguridad de las comunicaciones**
13.1		Instalaciones de gestión de la seguridad de la red.
13.1.1	8.20	Controles de red
13.1.2	8.21	Seguridad de los servicios de red
13.1.3	8.22	Separación en las redes
13.2		Transferencia de información;
13.2.1	5.14	Políticas y procedimientos de transferencia de información
13.2.2	5.14	Acuerdos sobre la transferencia de información
13.2.3	5.14	Mensajería electrónica
13.2.4	6.6	Acuerdos de confidencialidad o no divulgación
14		**Adquisición, desarrollo y mantenimiento del sistema**
14.1		Requisitos de seguridad de los sistemas de información
14.1.1	5.8	Análisis y especificación de los requisitos de SI
14.1.2	8.26	Seguridad de los servicios de aplicaciones en las redes públicas
14.1.3	8.26	Protección de las transacciones de los servicios de aplicación
14.2		Seguridad en los procesos de desarrollo y apoyo
14.2.1	8.25	Política de desarrollo segura
14.2.2	8.32	Procedimientos de control de cambios del sistema
14.2.3	8.32	Revisión técnica de las aplicaciones tras los cambios de plataforma operativa
14.2.4	8.32	Restricciones a los cambios en los paquetes de software
14.2.5	8.27	Principios de ingeniería de sistemas seguros
14.2.6	8.31	Entorno de desarrollo seguro
14.2.7	8.30	Desarrollo tercerizado
14.2.8	8.29	Pruebas de seguridad del sistema
14.2.9	8.29	Pruebas de aceptación del sistema
14.3		Datos de prueba
14.3.1	8.33	Protección de los datos de prueba
15		**Relaciones con los proveedores**
15.1		SI en las relaciones con los proveedores
15.1.1	5.19	Política de SI para las relaciones con los proveedores
15.1.2	5.20	Abordar la seguridad en los acuerdos con los proveedores
15.1.3	5.21	Cadena de suministro de tecnologías de la información y la comunicación
15.2		Gestión de la prestación de servicios de los proveedores
15.2.1	5.22	Seguimiento y revisión de los servicios de los proveedores
15.2.2	5.22	Gestión de los cambios en los servicios de los proveedores
16		**Gestión e incidentes de SI**
16.1		Gestión de incidentes y mejoras en la SI
16.1.1	5.24	Responsabilidades y procedimientos
16.1.2	6.8	Notificación de sucesos relacionados con la SI

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.

ISO/IEC 27002:2013	ISO/IEC 27002:2022	Nombre de control de acuerdo con la norma ISO/IEC 27002:2013
16.1.3	6.8	Notificación de deficiencias en la SI
16.1.4	5.25	Evaluación y decisión sobre eventos de SI
16.1.5	5.26	Respuesta a los incidentes de SI
16.1.6	5.27	Aprendizaje de los incidentes de SI
16.1.7	5.28	Recopilación de pruebas
17		**Aspectos de la SI en la gestión de la continuidad de la actividad**
17.1		Continuidad de la SI
17.1.1	5.29	Planificación de la continuidad de la SI
17.1.2	5.29	Implementación de la continuidad de la SI
17.1.3	5.29	Verificación, revisión y evaluación de la continuidad de la SI
17.2		Redundancias
17.2.1	8.14	Disponibilidad de instalaciones para el 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
18.1.3	5.33	Protección de los registros
18.1.4	5.34	Privacidad y protección de la información personal identificable
18.1.5	5.31	Regulación de los controles cifrados
18.2		Revisiones de la SI
18.2.1	5.35	Revisión independiente de la SI
18.2.2	5.36	Cumplimiento de las políticas y normas de seguridad
18.2.3	5.36, 8.8	Revisión del cumplimiento técnico

Nota:
Este material es una interpretación de SGS Academy con fines académicos y no pretende superar o reemplazar al estándar original.