

Lead Implementer Security Controls 27002:2022

Training Material



Tactical Compliance Badges

Idioma: Español

Ver:2026

Creado por: Valfra It Consulting.

ISO/IEC 27002:2022



Quien es Valfra It Consulting

Empresa 100% mexicana, fundada en 2009.

Somos el mejor equipo de profesionales creando un concepto innovador en servicios de consultoría, auditoría, capacitación y certificación, buscando reunir el mejor talento de profesionales para ofrecer servicios de excelencia en las mejores prácticas y sistemas de gestión en México, Canadá, EUA y Latinoamérica.

Líderes en implementación de mejores prácticas y sistemas de gestión, somos asesores reconocidos gracias a la calidad de nuestro servicio.

Miembros de la red de empresas Dun & Bradstreet somos reconocidos internacionalmente por las organizaciones fijadoras de estándares con mayor influencia del mundo, más de 50 asociaciones comerciales e industriales, el Gobierno Federal de Estados Unidos y las Naciones Unidas, entre otras instituciones.

Diamond partners de CERTIPROF LLC® organismo internacional para evaluar y certificar competencias a nivel mundial; VALFRA IT CONSULTING ha capacitado y certificado a cientos de profesionistas en normas internacionales como ISO 27001, ISO 22301, ISO 20000, ISO 9000 y mejores prácticas como Ciberseguridad, ITIL, SCRUM, NIST y NICE.



Valor y Experiencia

Con 17 años de experiencia hemos desarrollado, compartido conocimiento y experiencias en cuanto al conjunto de las prácticas más actuales, con la finalidad que las TI cumplan su propósito y objetivo.

Nuestra misión

Convertirnos en su socio de negocio y aliado estratégico.



Nuestras Afiliaciones



Badge Digital



Los Badges digitales contienen información sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.

Permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global, los perfiles de LinkedIn con insignias digitales reciben más atención por parte de reclutadores y empleadores.

Se reportó que esto mejoró su credibilidad profesional en sus redes. Además, que los Badges digitales les ayudan a identificar rápidamente habilidades específicas.

Se ha demostrado que incluirlos en currículums genera más de probabilidades de contratación en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.



Badge Digital



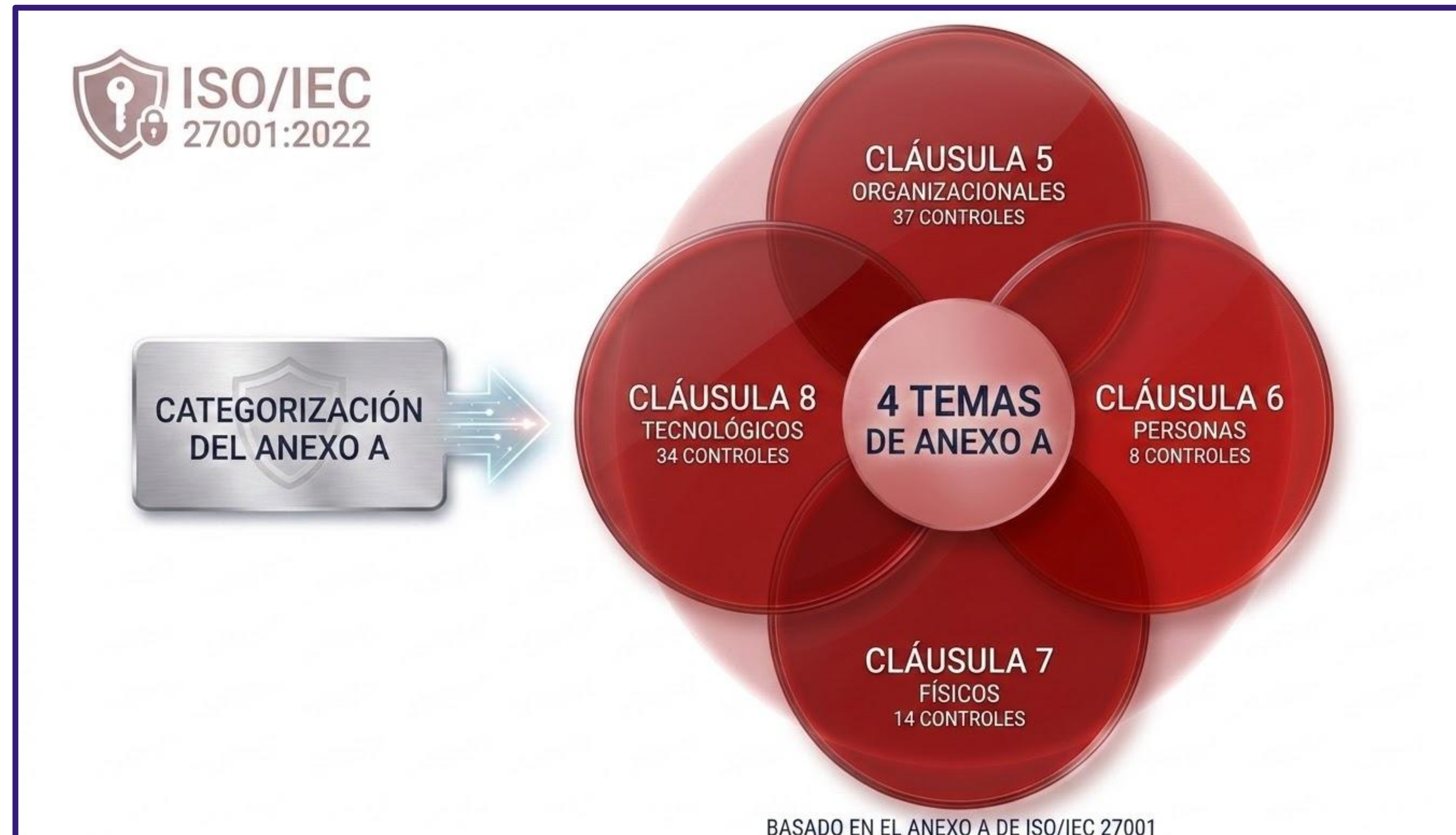
Los Certificados de Cumplimiento Táctico **Lead Implementer Security Controls 27002:2022** (complemento de los Certificados Lead Implementer 27001:2022) demuestran que las personas cuentan con las competencias necesarias en la implementación de los 93 controles de seguridad dentro de un sistema de gestión de seguridad de la información (SGSI) en apego a las normas ISO/IEC 27002:2022.



Introducción al curso

Estructura del Anexo A

El Rol Lead Implementer Security Controls es un complemento al Rol Lead Implementer para desarrollar competencias en Implementación de los 93 controles del **anexo A** en apego a la norma ISO/IEC 27002:2022.



Introducción al curso

Estructura del Anexo A

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

- a) Dentro del contexto de un sistema de gestión de seguridad de la información (SGSI) basado en ISO IEC 27001.
- b) Para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente.
- c) Para desarrollar directrices de gestión de la seguridad de la información específicas de la organización.



Norma ISO/IEC 27002:2022

INTERNATIONAL
STANDARD

ISO/IEC
27002

Third edition
2022-02

Information security, cybersecurity
and privacy protection — Information
security controls

Sécurité de l'information, cybersécurité et protection de la vie
privée — Mesures de sécurité de l'information

Norma que establece un conjunto de controles de seguridad de la información, ciberseguridad y protección de la privacidad, diseñados para ser utilizados como referencia por organizaciones de cualquier tipo y tamaño. Esta edición reemplaza a la de 2013, presentando cambios técnicos, una estructura revisada con una nueva taxonomía y la incorporación de atributos para categorizar los controles.

 **Objetivo Principal:** Servir como una guía de referencia para que las organizaciones seleccionen, implementen y gestionen controles de seguridad de la información dentro del marco de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022.



Clausulado Norma ISO/IEC 27002:2022



1. Objeto y campo de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Estructura de este documento
5. Controles organizacionales
6. Controles de personas
7. Controles físicos
8. Controles tecnológicos

Anexo A Atributos de Control

Anexo B (B1 y B2) Mapeo de Controles Vs ISO 27002:2013.



1. Objeto y campo de aplicación

1. Definición Textual y Propósito General

El objeto principal de esta norma es proporcionar un catálogo genérico de controles de seguridad de la información, incluyendo directrices para su implementación.

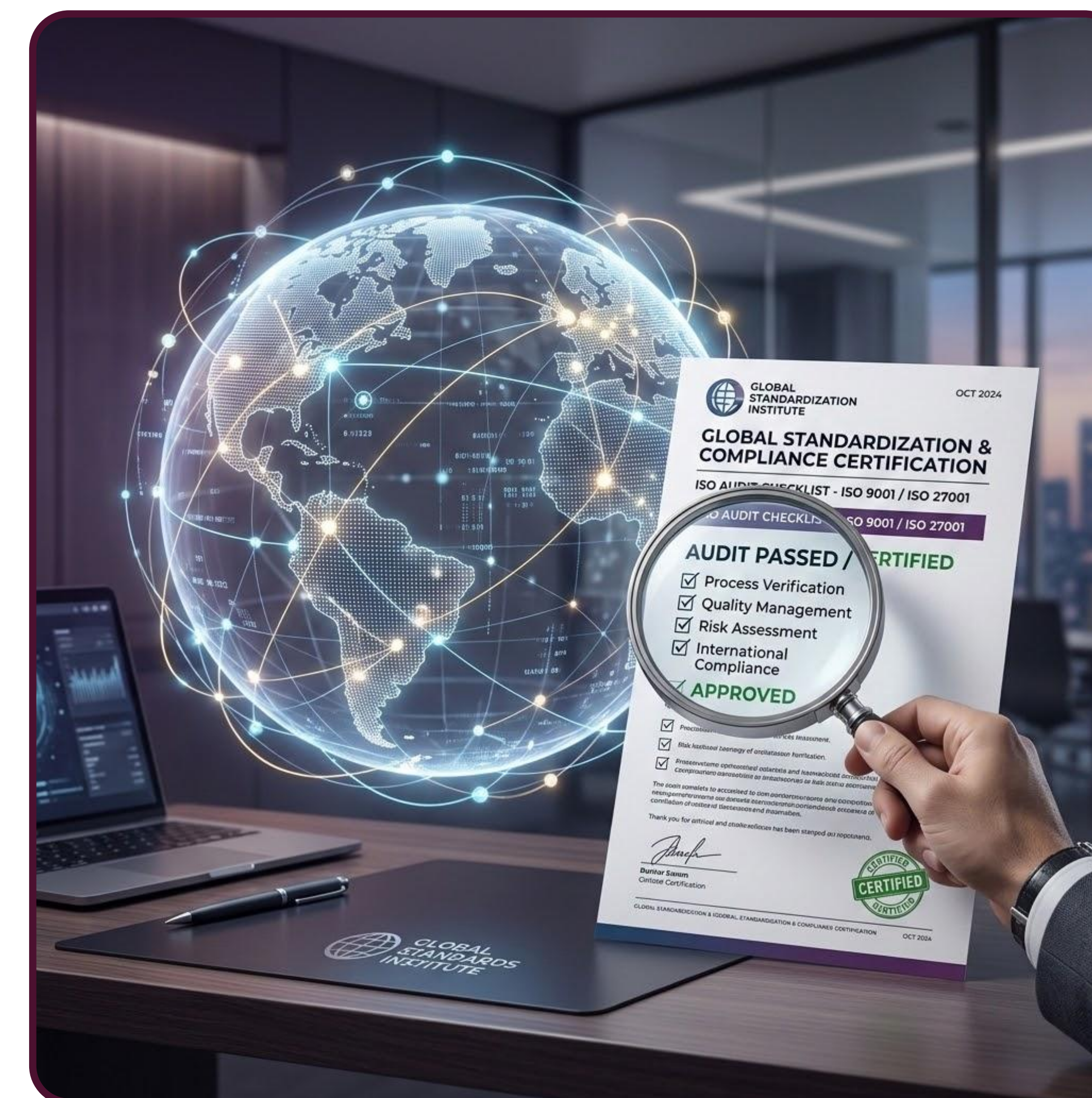
A diferencia de la ISO 27001, esta cláusula deja claro que la norma ISO 27002 no establece requisitos obligatorios, sino que sirve como un documento de referencia (una guía de buenas prácticas) para que las organizaciones elijan las salvaguardas que mejor se adapten a sus riesgos específicos.

2. Componentes Clave del Campo de Aplicación

La Cláusula 1 establece que el documento está diseñado para ser utilizado por organizaciones de todo tipo. Sus objetivos de aplicación específicos son:

Selección de controles: Ayudar a las organizaciones a elegir los controles adecuados durante el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001.

Implementación de buenas prácticas: Servir como guía para implementar controles de seguridad de la información reconocidos a nivel internacional.



1. Objeto y campo de aplicación

Desarrollo de pautas propias: Facilitar que sectores específicos (como el sector salud, financiero o gubernamental) o las propias empresas desarrollen sus propias directrices de gestión de la seguridad, utilizando estos 93 controles como base común.

3. ¿A quién va dirigida? (Universalidad)

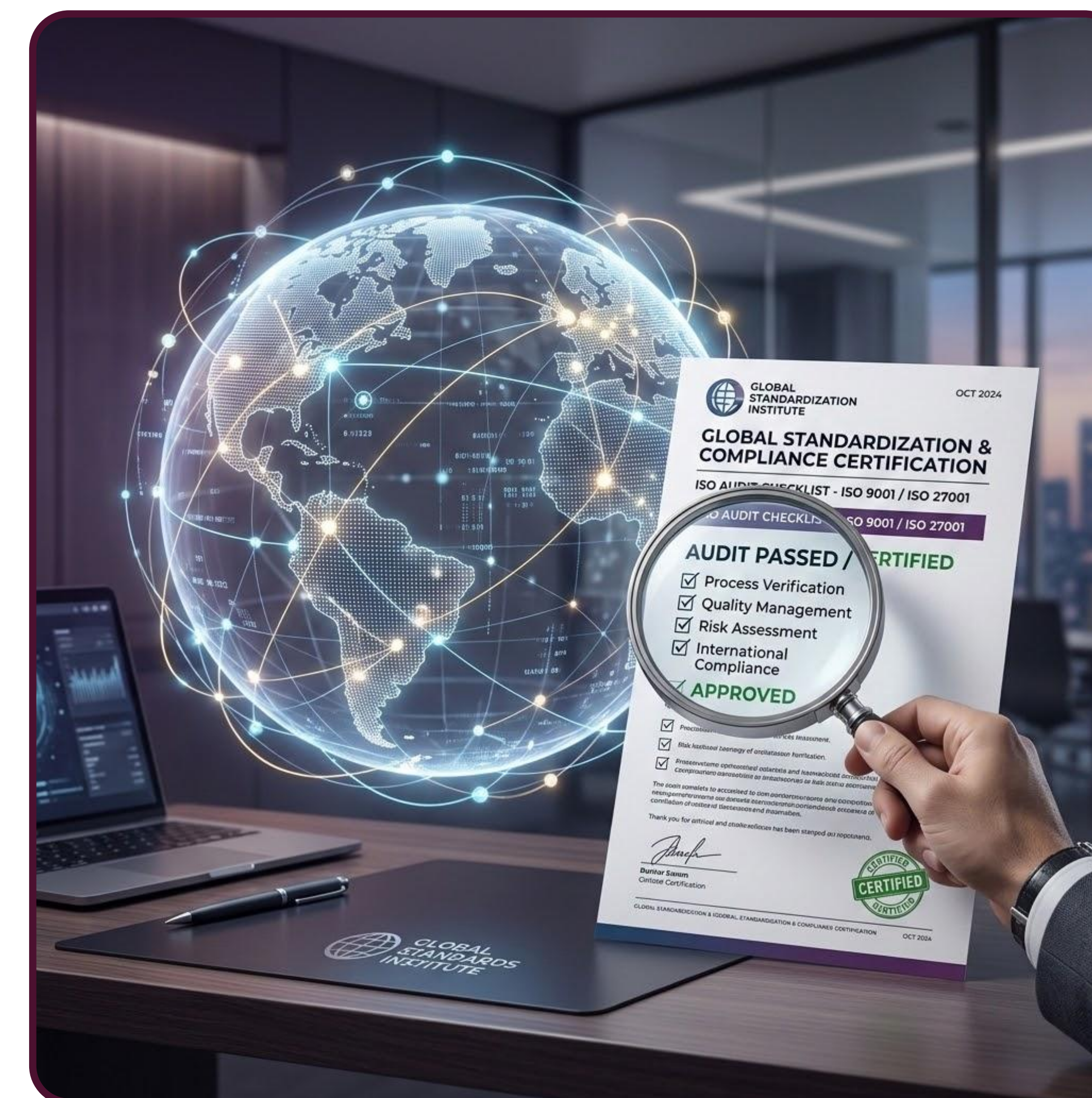
La norma especifica explícitamente que sus directrices son universales. Esto significa que el campo de aplicación abarca a:

- Cualquier tipo de organización: Empresas privadas, entidades públicas, organizaciones sin fines de lucro (ONGs).
- Cualquier tamaño: Desde microempresas y Startups hasta corporaciones multinacionales.
- Cualquier sector o industria: Tecnología, salud, manufactura, finanzas, educación, etc.

4. Relación con la Certificación y la ISO 27001

Un punto crítico implícito en el objeto y campo de aplicación es la naturaleza **no certificable** de la ISO 27002 por sí sola.

ISO 27002 (La Guía): Detalla el Anexo A. Su campo de aplicación es ser la herramienta de implementación detallada; se deben considerar temas relacionados como exclusiones y auditorías.

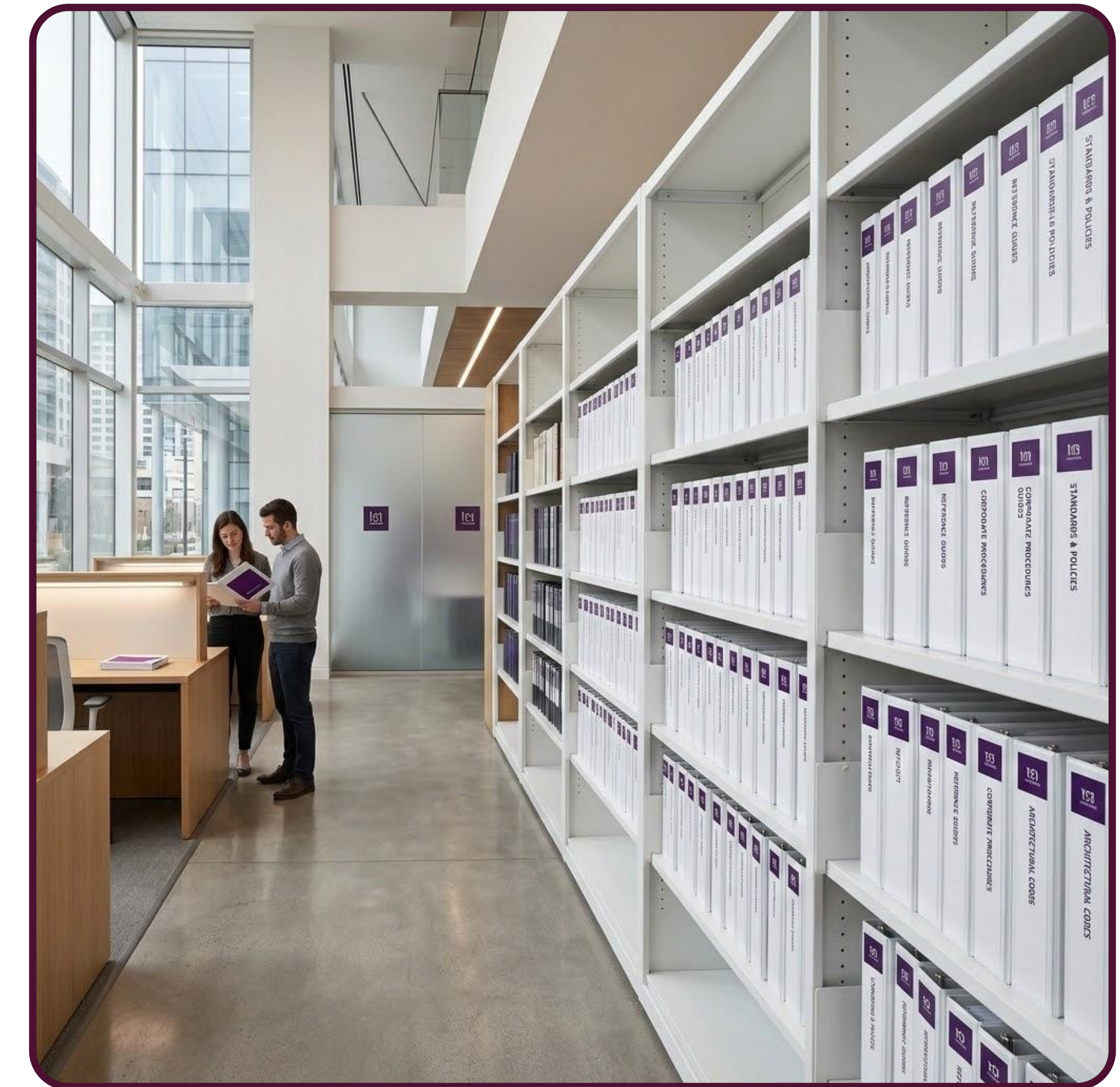


2. Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que parte o la totalidad de su contenido constituye requisitos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento de referencia (incluida cualquier enmienda).

A continuación, se cita la única referencia normativa obligatoria:

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Tecnologías de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Visión general y vocabulario).

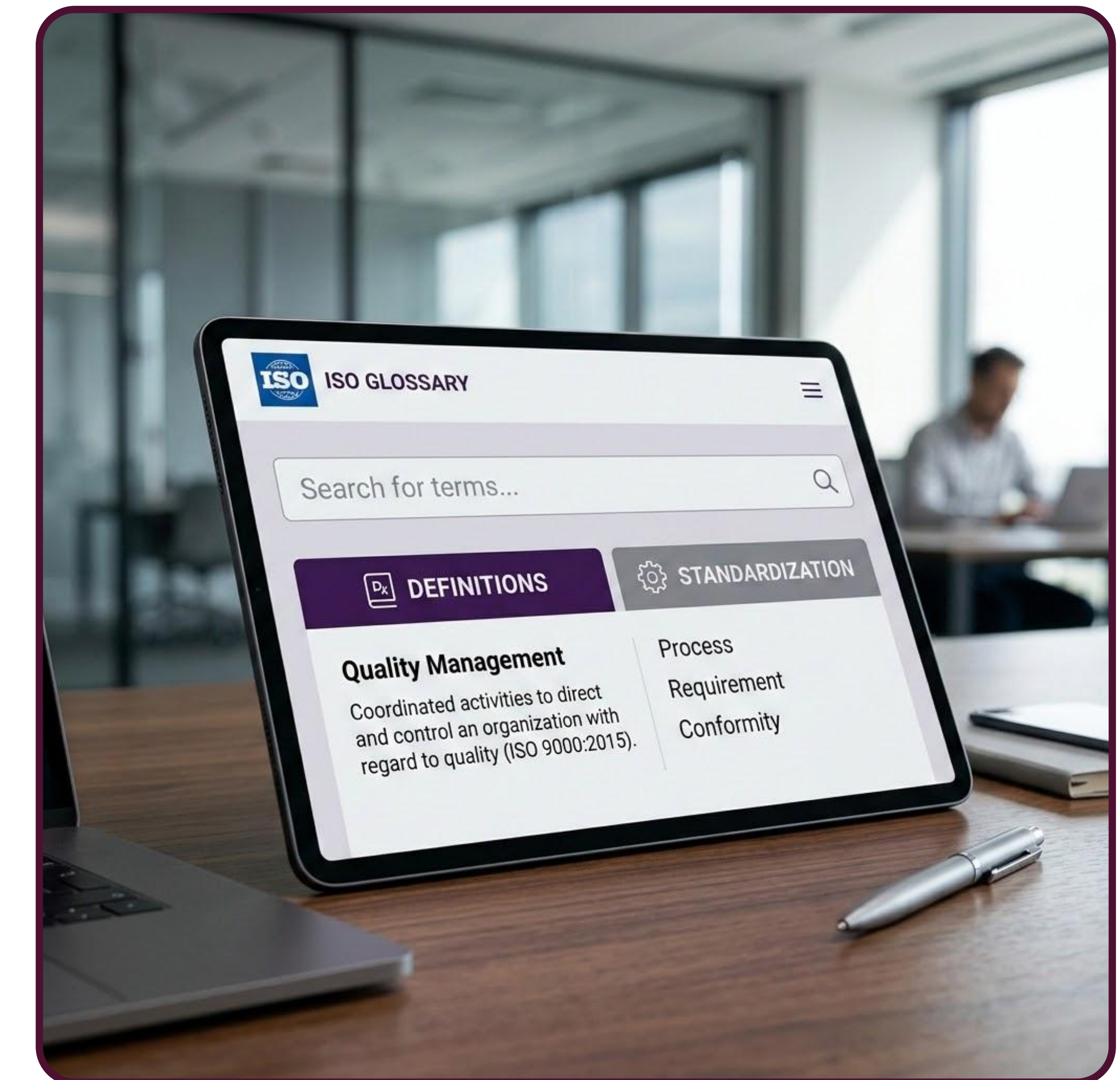


3. Términos y definiciones

La Cláusula 3: Términos y definiciones (Terms and definitions) de la norma ISO/IEC 27002:2022 es el puente conceptual que asegura que organizaciones de todo el mundo, sin importar su idioma, país o sector, hablen exactamente el mismo lenguaje técnico cuando implementan seguridad de la información.

Al igual que en la cláusula anterior, la norma comienza indicando formalmente que para los efectos de este documento, se aplican los términos y definiciones dados en la ISO/IEC 27000.

Sin embargo, debido a la gran modernización que sufrió la versión 2022 (con la llegada de la nube, la inteligencia de amenazas y la ciberseguridad avanzada), la Cláusula 3 define de manera específica algunos términos clave que son vitales para entender cómo aplicar los 93 controles.



4. Estructura del documento

Es el mapa de navegación de todo el estándar. Esta sección no contiene controles en sí misma, sino que explica cómo leer, entender y aplicar los 93 controles de seguridad que vienen en los capítulos siguientes.

A continuación, se desarrolla en detalle los componentes fundamentales que introduce esta cláusula:

- Los Tres Elementos de un Control (La Estructura de un control):

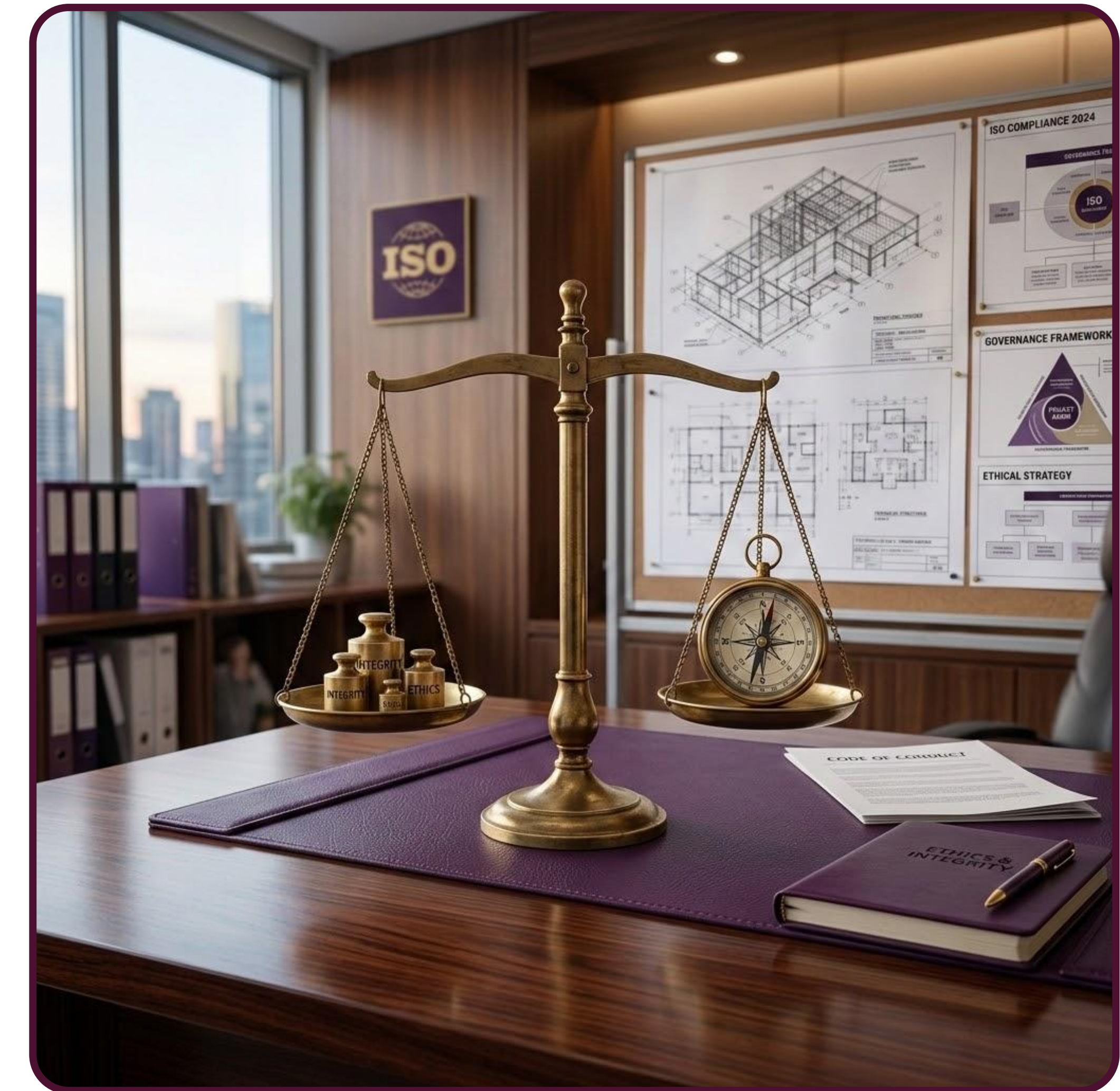
Tabla de Atributos: Una matriz al inicio de cada control que lo clasifica mediante etiquetas (metadatos).

El Control: La declaración específica de la medida de seguridad que se debe implementar.

Resumen de las Directrices de Implementación: El texto detallado que explica cómo poner en marcha dicho control, ofreciendo ejemplos, procesos recomendados y mejores prácticas.

Otra Información: Notas adicionales, referencias cruzadas a otras normas o consideraciones legales/técnicas que ayudan a su comprensión.

- El Sistema de Atributos (**Anexo A**)



4. Estructura del documento

- Las 4 Grandes Categorías de Controles (Temáticas)

En lugar de los antiguos 14 dominios de la versión 2013, la Cláusula 4 explica que los 93 controles actuales se agrupan de manera mucho más natural en solo 4 secciones temáticas:

Cláusula 5. Controles organizacionales: Políticas, gestión de riesgos, relaciones con proveedores, etc.

Cláusula 6. Controles de personas: Concienciación, acuerdos de confidencialidad, teletrabajo.

Cláusula 7. Controles físicos: Perímetros de seguridad, oficinas, protección del equipamiento.

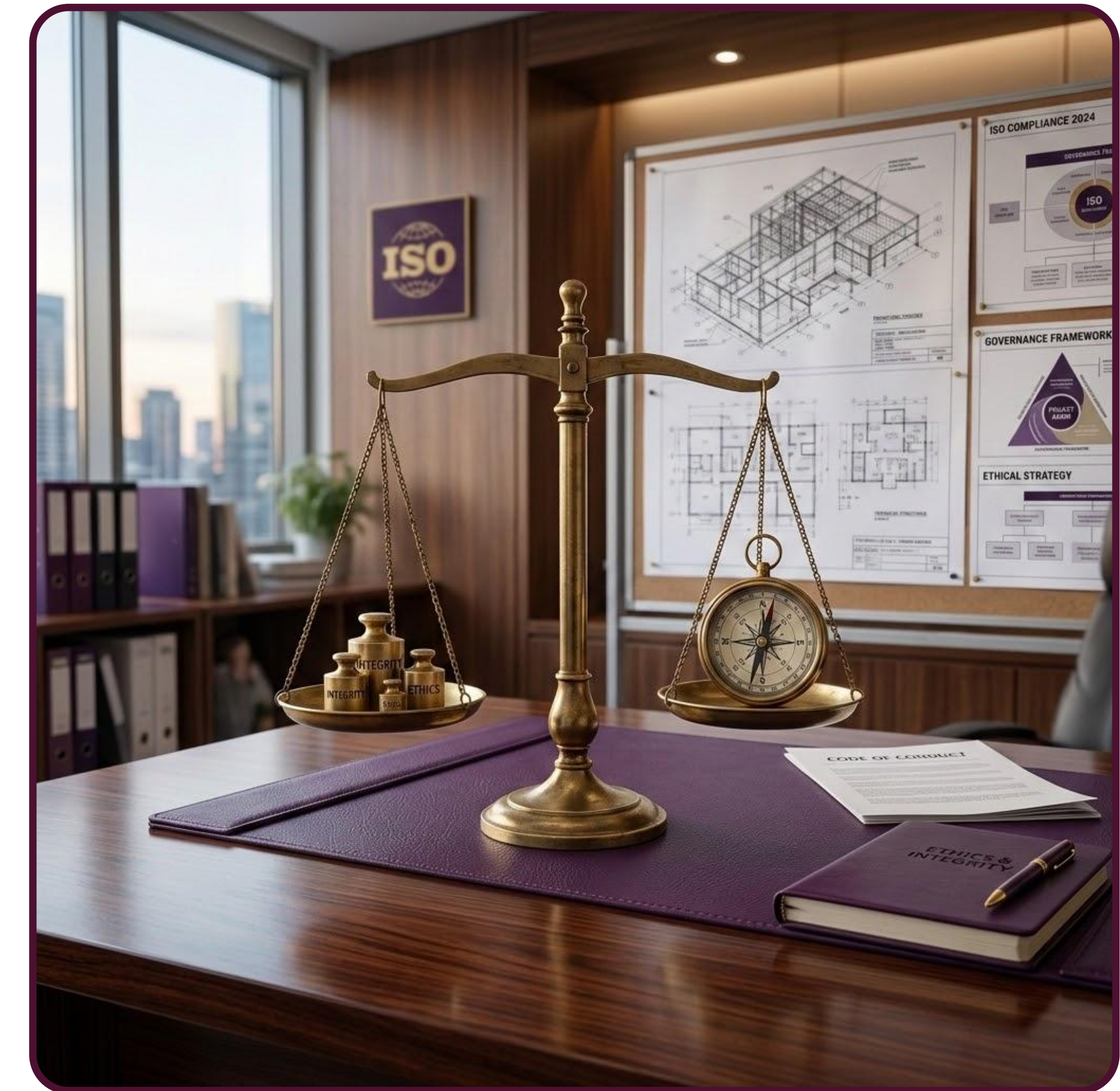
Cláusula 8. Controles tecnológicos: Cifrado, redes, desarrollo seguro, autenticación.

- Principios para una Aplicación Práctica y Flexible.

La Cláusula 4 cierra con una serie de directrices de sentido común para las empresas.

No todos los controles aplican a todos: La norma es un menú de opciones. Las organizaciones deben elegir qué controles aplicar basándose estrictamente en su propia Evaluación de Riesgos.

Personalización: Las Resumen de las Directrices de Implementación son recomendaciones generales. Cada empresa puede y debe adaptarlas a su presupuesto, tecnología y cultura corporativa.



Anexo A (Aplica cláusulas siguientes)

El Anexo A (Informativo) de la ISO 27002:2022 detalla las directrices para la aplicación de los Atributos. La norma define este sistema para que las organizaciones puedan etiquetar y categorizar sus controles, facilitando la creación de vistas personalizadas para diferentes audiencias (como la alta dirección, auditores o el equipo técnico).

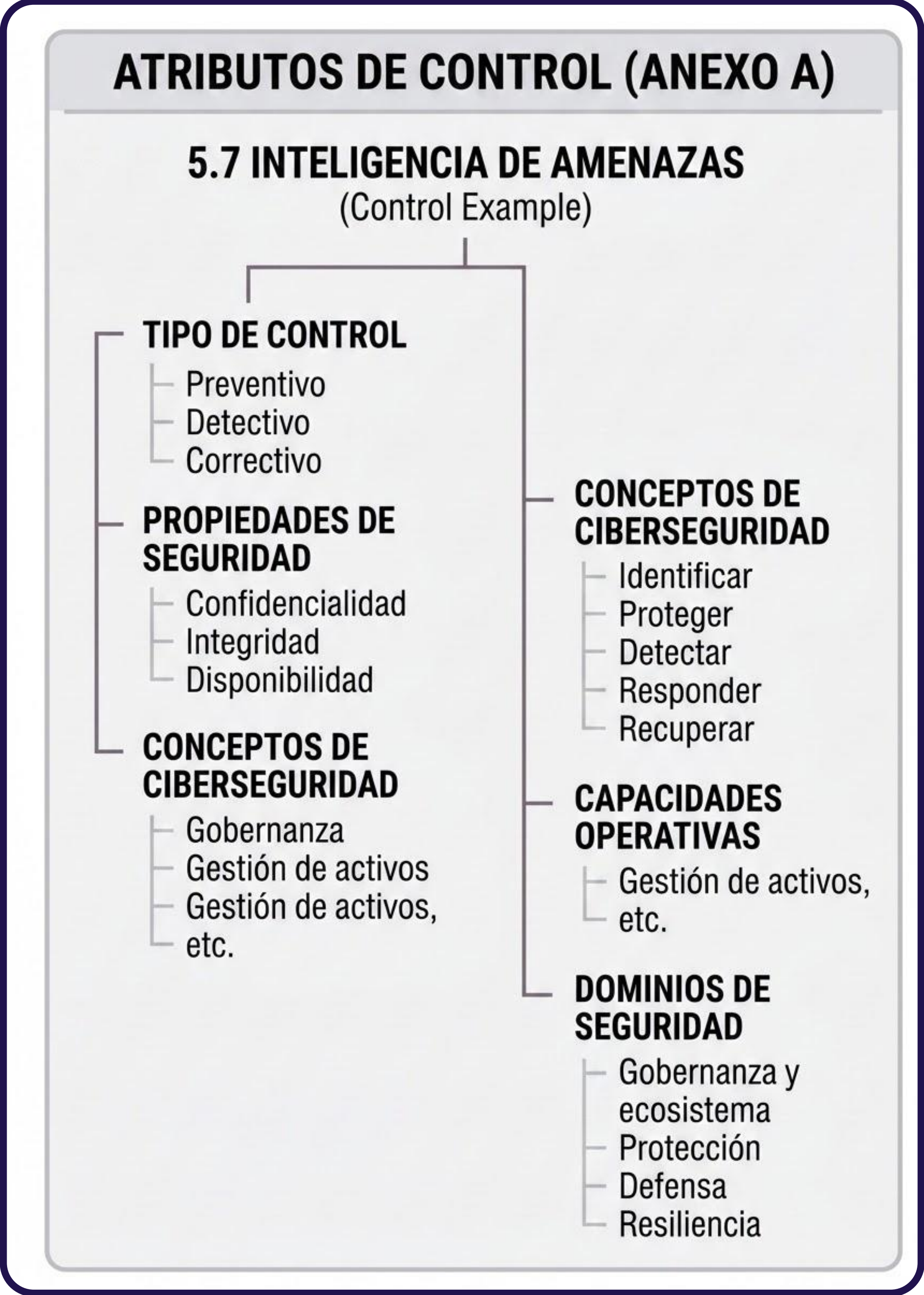
- **El Sistema de Atributos (La gran innovación del 2022)**

El principio general más revolucionario de la versión 2022 es la introducción de los Atributos. La Cláusula 4 define un conjunto de 5 categorías de atributos que permiten a las organizaciones "filtrar" y ordenar los controles según sus necesidades operativas:

A. Tipo de Control (Control Type)

Clasifica el control según el momento en que actúa frente a un riesgo:

- Preventivo:** Diseñado para evitar que ocurra un incidente (ej. una contraseña robusta).
- Detectivo:** Diseñado para actuar cuando ocurre un incidente (ej. una alarma o un log de errores).
- Correctivo:** Diseñado para responder y recuperar tras un incidente (ej. copias de seguridad/backups).



Anexo A (Aplica cláusulas siguientes)

B. Propiedades de la Seguridad de la Información (Information Security Properties)

Vincula el control con los pilares de la tríada CID:

- Confidencialidad
- Integridad
- Disponibilidad

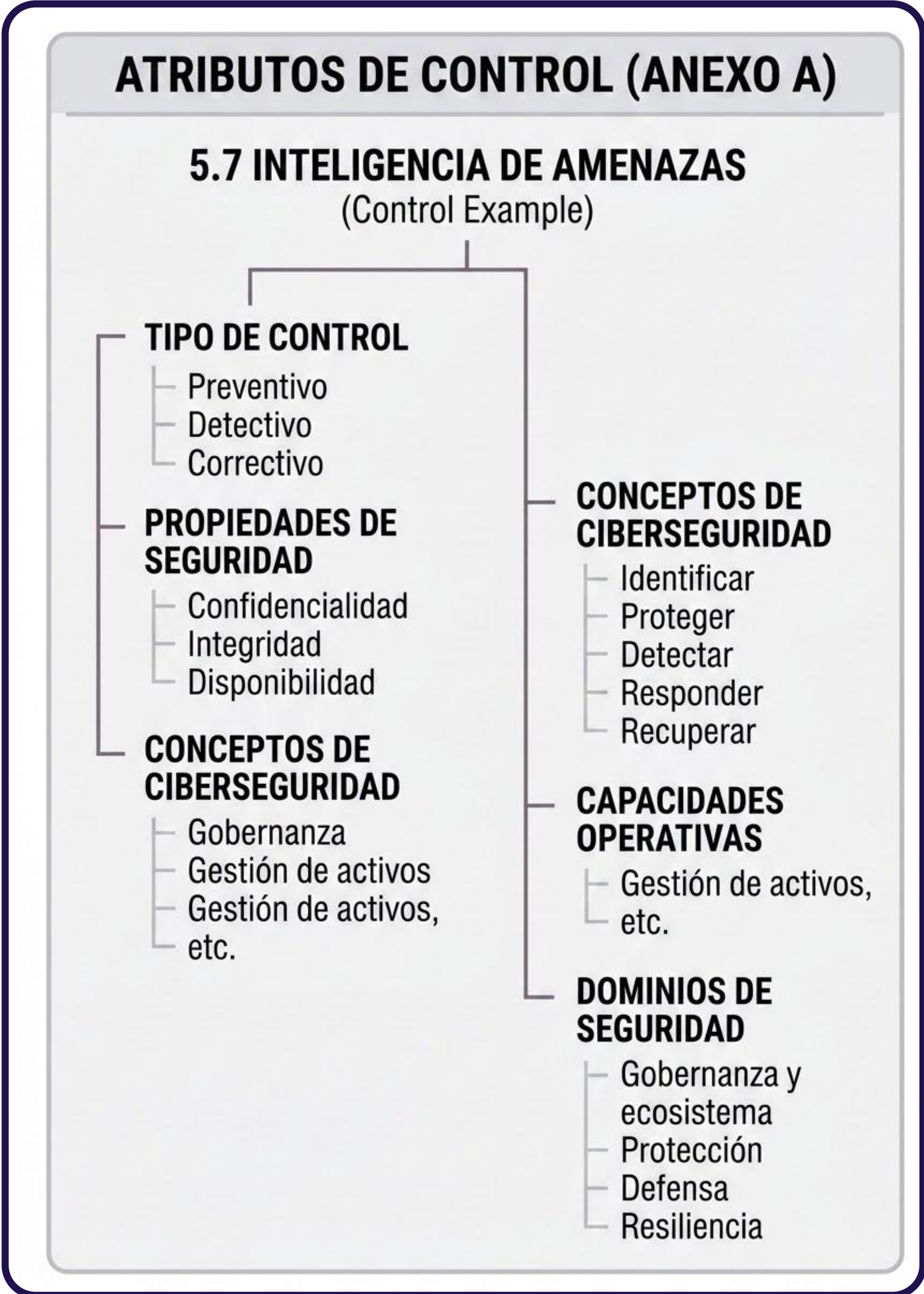
C. Conceptos de Ciberseguridad (Cybersecurity Concepts)

Alinea los controles con la taxonomía de marcos internacionales como el NIST CSF:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

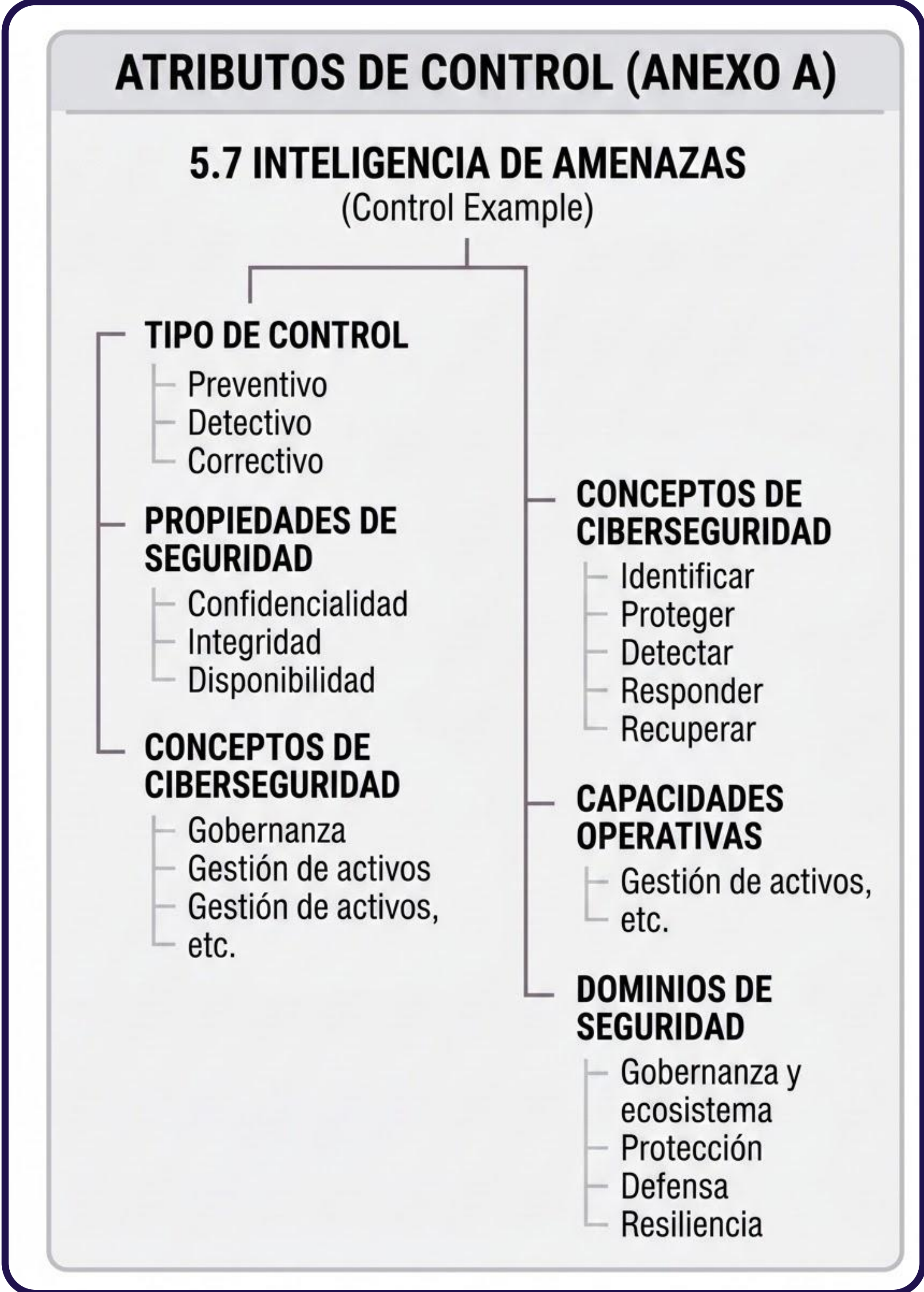
D. Capacidades Operativas (Operational Capabilities)

Clasifica el control según el área profesional o técnica que debe hacerse cargo de él dentro de la empresa:



Anexo A (Aplica cláusulas siguientes)

- Governance
- Asset_management
- Governance
- Asset_management
- Information_protection
- Human_resource_security
- Physical_security
- System_and_network_security
- Application_security,
- Secure_configuration,
- Identity_and_access_management,
- Threat_and_vulnerability_management,
- Continuity,
- Supplier_relationships_security,
- Legal_and_compliance,
- Information_security_event_management,
- Information_security_assurance)
- Information_protection
- Human_resource_security,



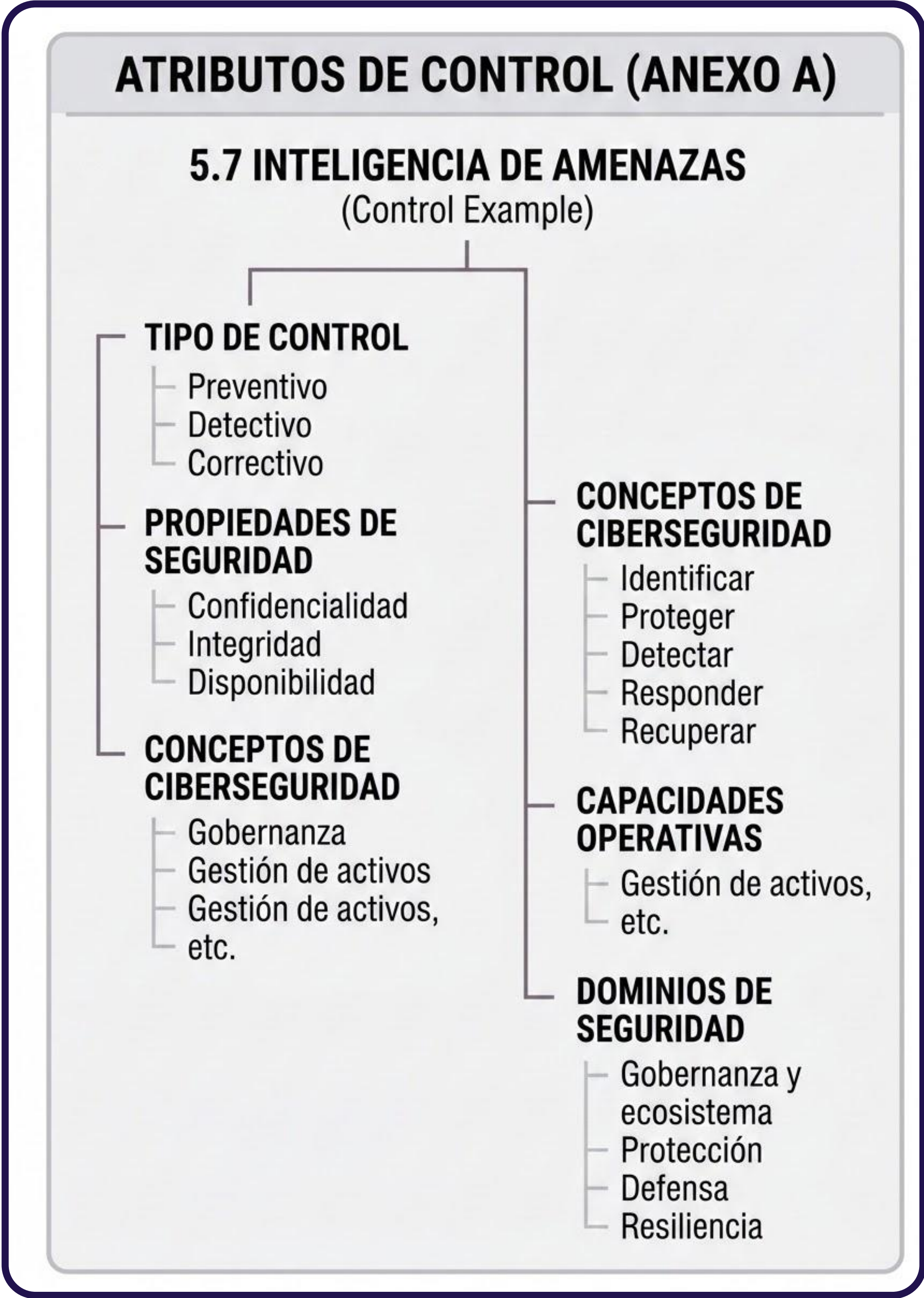
Anexo A (Aplica cláusulas siguientes)

- Physical_security
- System_and_network_security
- Application_security,
- Secure_configuration,
- Identity_and_access_management
- Threat_and_vulnerability_management
- Continuity,
- Supplier_relationships_security
- Legal_and_compliance,
- Information_security_event_management
- Information_security_assurance

E. Dominios de Seguridad (Security Domains)

Divide los controles según el área de experiencia técnica

- Gobernanza y Ecosistema
- Protección
- Defensa
- Resiliencia.

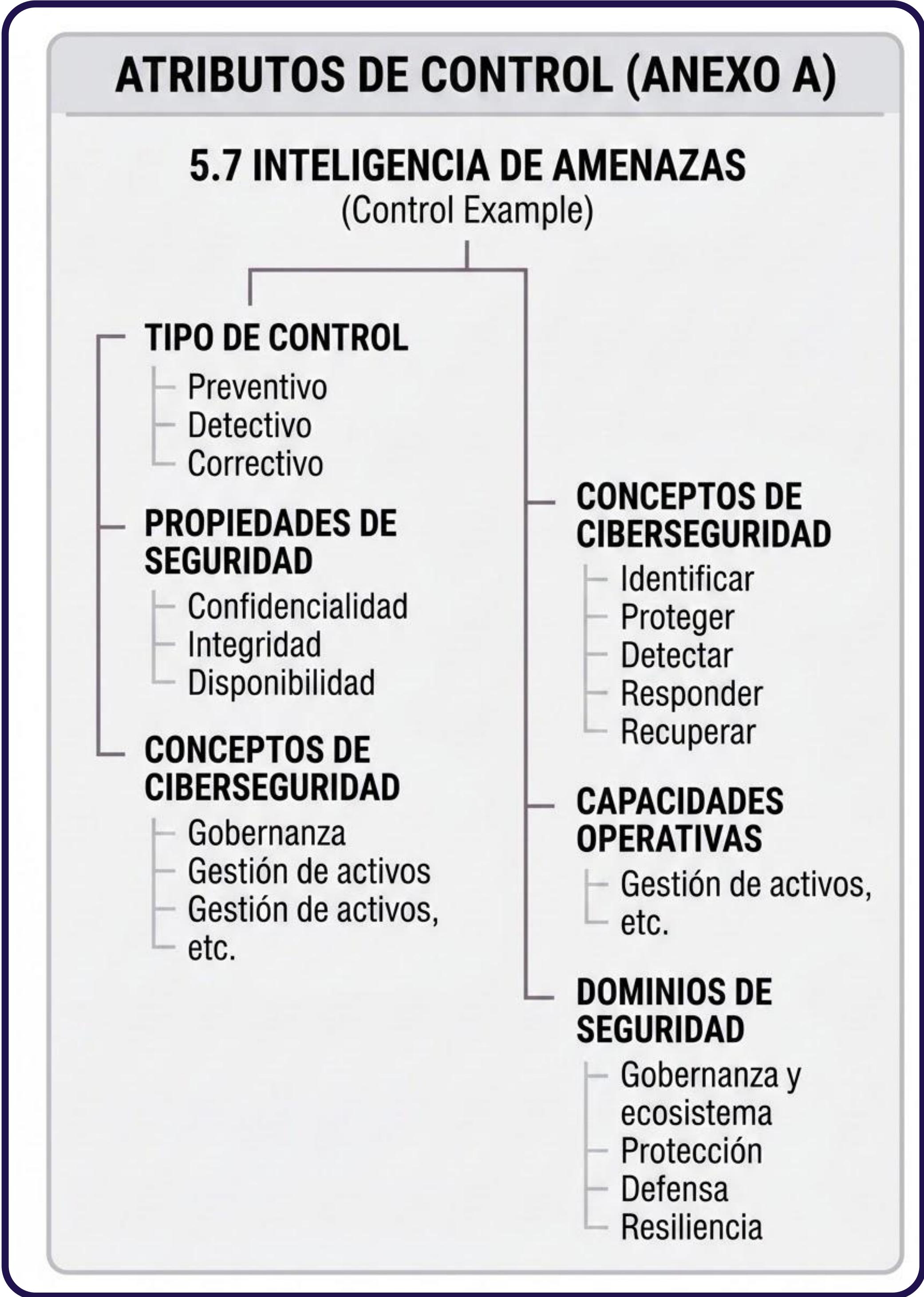


Anexo A (Aplica cláusulas siguientes)

Anexo A.1

Es una matriz de todos los controles con sus atributos:

Table A.1 — Matrix of controls and attribute values						
ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosys- tem #Resil- ience



Cláusula 5: Controles organizacionales

Control 5.1 Políticas para la seguridad de la información

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

- **Control:** La política de seguridad de la información y las políticas específicas del tema deben ser revisadas y aprobadas por la dirección, publicadas y comunicadas a los empleados y a las partes interesadas pertinentes y revisadas a intervalos planificados y si ocurren cambios significativos.
- **Resumen de las Directrices de Implementación:** Este control actúa como la base de todo el Sistema de Gestión de Seguridad de la Información (SGSI). Las directrices se centran en cómo estructurar, aprobar y mantener vivas estas políticas:
 - Nivel Superior vs. Políticas Específicas:** Debe existir una Política de Seguridad de la Información de alto nivel (aprobada por la alta dirección) que defina la dirección, el compromiso y los objetivos generales de la organización (Validar caso: **Cuando una organización opera en más de una -localidad con leyes y regulaciones diferentes**). Por debajo de esta, se deben desarrollar políticas específicas por tema (por ejemplo: control de acceso, trabajo remoto, clasificación de la información, uso de activos).
 - Aprobación y Publicación:** Toda política debe tener un dueño definido y contar con la aprobación formal de la dirección antes de ser distribuida y debe estar disponible en un formato accesible.
 - Comunicación y Concientización:** No basta con publicarlas. Se deben comunicar de manera clara, comprensible y relevante para los empleados y contratistas externos. Es fundamental integrarlas en los programas de capacitación.
 - Revisión Continua:** Las políticas deben revisarse en periodos de tiempo definidos (ej. anualmente) o cuando ocurran cambios significativos (cambios en regulaciones, incidentes graves de seguridad, nuevas tecnologías o cambios estructurales en la empresa).



Cláusula 5: Controles organizacionales

Control 5.1 Políticas para la seguridad de la información

- Otra Información

Alineación Estratégica: Las políticas de seguridad no deben crearse de forma aislada; deben estar alineadas con la estrategia de negocio, la gestión de riesgos general de la empresa y los requisitos legales/contractuales aplicables (como GDPR, regulaciones financieras locales, etc.).

Consecuencias: La norma sugiere que las políticas incluyan o hagan referencia a las consecuencias o acciones disciplinarias en caso de incumplimiento, para asegurar su obligatoriedad.

💡 Implementar el control 5.1 no se trata de redactar un PDF de 80 páginas que nadie va a leer solo para pasar una auditoría. Aquí van unos consejos prácticos "del mundo real" para que tus políticas funcionen de verdad:

-Adiós al "Abogado", hola a la claridad: Redacta con un lenguaje directo, amigable y utiliza ejemplos cotidianos.

-Centraliza y versiona (El síndrome del PDF viejo): Asegúrate de tener un único "origen de la verdad" (SharePoint, Confluence, etc.). Si permites que la gente descargue las políticas, en seis meses la mitad de la empresa estará usando versiones obsoletas.

-Mide la lectura, no solo el envío: Utiliza herramientas que requieran una firma digital de aceptación o implementa un micro-cuestionario (quiz) de 3 preguntas al final de la lectura para asegurar la comprensión.

-Automatiza la revisión: No confíes en la memoria. Programa alertas automáticas en el calendario del comité de seguridad para revisar las políticas cada 10 u 11 meses. Es mejor corregir pequeños detalles sobre la marcha que reescribir todo bajo presión antes de la auditoría de certificación.



Cláusula 5: Controles organizacionales

Control 5.2 Roles y responsabilidades de seguridad de la información

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

- **Control:** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización
- **Resumen de las Directrices de Implementación:** Este control busca eliminar la ambigüedad de "quién hace qué" en materia de seguridad, que no queden brechas de responsabilidad sin cubrir:
 - Definición y Asignación Clara:** Se deben definir explícitamente las responsabilidades de seguridad para todo el personal. Esto incluye tanto las responsabilidades generales de todo empleado como las especializadas (ej. el rol de CISO o administradores de red).
 - Segregación de Funciones:** Al asignar roles, se debe considerar el principio de segregación de funciones (ligado al control 5.3) para evitar conflictos de interés (por ejemplo, que la misma persona que desarrolla un código sea quien apruebe su paso a producción sin supervisión).
 - Autorización e Identificación:** Los roles con privilegios especiales o acceso a información crítica deben estar claramente identificados y autorizados formalmente por la dirección.
 - Competencia y Capacitación:** Las personas asignadas a roles específicos deben contar con el conocimiento, las habilidades y los recursos para ejecutar sus funciones de manera efectiva.



Cláusula 5: Controles organizacionales

Control 5.2 Roles y responsabilidades de seguridad de la información

- Otra Información

Sponsor Político (Alta Dirección): Aunque se deleguen las tareas operativas a un equipo de seguridad (CISO, analistas, etc.), la responsabilidad última (accountability) del éxito o fracaso del SGSI recae siempre en la alta dirección de la organización.

Actualización: Los roles y responsabilidades deben actualizarse inmediatamente cuando ocurran cambios organizacionales, como reestructuraciones internas, despidos o fusiones.

💡 Si la seguridad de la información es "tarea de todos", muchas veces termina siendo "tarea de nadie". Para evitar que esto pase en tu organización, te sugiero lo siguiente:

-Complementa con una Matriz RACI: No te limites a describir los roles en un documento de texto aburrido.

-Evita el "CISO de papel": Es muy común en empresas medianas asignar el rol de Responsable de Seguridad al Director de TI o a un administrador de sistemas solo para llenar el requisito. Si haces esto, asegúrate de que esa persona tenga el tiempo real, el presupuesto y la autoridad para tomar decisiones de seguridad, y que su evaluación de desempeño no dependa exclusivamente de "que los sistemas estén encendidos" (disponibilidad), sino también de que estén protegidos.

-Modifica los perfiles de puesto oficiales (Job Descriptions): Las responsabilidades de seguridad no deben vivir únicamente en el manual de ISO. Deben estar integradas formalmente en los contratos de trabajo o en las descripciones de cargo que Recursos Humanos utiliza para contratar y evaluar al personal.

-Cuidado con los "Superusuarios" multifuncionales (Conflicto de interés): En organizaciones pequeñas, una sola persona suele configurar el firewall, dar de alta usuarios, revisar los logs y programar los respaldos. Si este es tu caso, documenta este riesgo y establece controles compensatorios.



Cláusula 5: Controles organizacionales

Control 5.3 Segregación de funciones

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

- **Control:** Las funciones en conflicto y las áreas de responsabilidad en conflicto deben estar segregadas.
- **Resumen de las Directrices de Implementación:** El objetivo principal de este control es reducir el riesgo de modificaciones no autorizadas, fraudes, errores o uso indebido de los activos de la organización mediante la división de tareas críticas:
 - Principio de Doble Control:** Ninguna persona debe tener la capacidad de iniciar, autorizar, ejecutar y verificar un proceso crítico de principio a fin sin la intervención de alguien más.
 - Identificación de Funciones en Conflicto:** Las organizaciones deben listar y analizar qué actividades, si las realiza un mismo usuario, representan un riesgo alto.
 -  **Controles Compensatorios:** En los casos donde la segregación de funciones sea imposible de implementar (por ejemplo, debido al tamaño pequeño de la empresa), se deben diseñar actividades de supervisión posteriores, auditorías frecuentes o registros de auditoría mejorados y protegidos para mitigar el riesgo.



Cláusula 5: Controles organizacionales

Control 5.3 Segregación de funciones

-  **Controles Compensatorios:** El concepto de controles compensatorios proviene originalmente del ámbito del control interno financiero y la auditoría contable y no de la informática o la ciberseguridad, como muchos creen hoy en día.

Su llegada a las Normas ISO (ISO 27001/27002): Sí un control de la norma ISO 27002 (como el 5.3 de Segregación de Funciones) no se puede aplicar por limitaciones técnicas, económicas o de tamaño de la empresa, la norma **PIDE** de manera implícita a buscar una alternativa que compense ese riesgo y reduzca la vulnerabilidad a un nivel aceptable.

 **¡Cuidado con la "Trampa" del Control Compensatorio!**, ISO no define “control compensatorio” ni declara una manera formal de implementar ni evaluar y no todos los controles son aptos para compensatorios.

En el mundo real, muchas organizaciones usan los controles compensatorios como una excusa para la flojera tecnológica u operativa. Dicen: "No vamos a implementar la autenticación de doble factor (MFA) porque los usuarios se quejan; en su lugar, nuestro control compensatorio será cambiar la contraseña cada 30 días".

-  **Controles Compensatorios, Postura ISO:** la palabra "compensatorio" sí aparece de forma literal en la guía de varios controles cuando la norma reconoce que el control ideal es imposible de cumplir.

"When segregation is difficult to achieve, compensating controls such as monitoring of activities, audit trails and management supervision should be considered."

(Cuando la segregación sea difícil de lograr, se deben considerar controles compensatorios tales como el monitoreo de actividades, pistas de auditoría y supervisión de la gestión).



Cláusula 5: Controles organizacionales

Control 5.3 Segregación de funciones

El "permiso" para usar un control compensatorio proviene de la Cláusula 6.1.3 (Tratamiento de los riesgos de seguridad de la información) de la ISO 27001.

La norma establece los siguientes pasos:

- La organización debe determinar las acciones para mitigar los riesgos identificados.
- La organización debe implementar los controles que considere necesarios.

- **Otra Información:**

Automatización del Control: La segregación no solo se logra mediante políticas en papel, la forma más efectiva de aplicarla es configurando técnicamente los sistemas informáticos mediante Matrices de Permisos y perfiles basados en el rol (RBAC - Role-Based Access Control), impidiendo que un usuario técnico acumule privilegios conflictivos.

💡 **No segregues todo, prioriza por criticidad:** Si intentas segregar cada pequeña tarea en tu organización, vas a paralizar la operación. Concéntrate exclusivamente en el "Dinero" (procesos financieros) y en la "Llave del Reino" (procesos core de TI y accesos de administración global).

💡 **El peligro del "Desarrollador-Administrador":** En el mundo del software y DevOps, es muy tentador que el programador tenga accesos totales a la base de datos de producción para "arreglar fallas rápido". Esto es un imán de incidentes. Implementa flujos de aprobación automáticos donde el despliegue a producción requiera el visto bueno de un par o de un líder de QA, y utiliza accesos temporales tipo Just-In-Time (JIT) si alguien requiere ingresar a producción en una emergencia.



Cláusula 5: Controles organizacionales

Control 5.4 Responsabilidades de la dirección

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

- **Control:** La dirección debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas específicas del tema y los procedimientos de la organización.
- **Resumen de las Directrices de Implementación:** Este control exige que los líderes de la empresa dejen de ser espectadores pasivos y pasen a ser los principales promotores de la seguridad, garantizando que el personal cumpla con sus obligaciones:
 - Predicar con el ejemplo (Tone at the top):** La dirección en todos los niveles (gerentes, directores, jefes de área) debe demostrar activamente su compromiso con la seguridad, siguiendo ellos mismos las políticas antes de exigirles a sus subordinados.
 - Asegurar la Concientización y Capacitación:** Es responsabilidad de los líderes garantizar que todo el personal a su cargo reciba la formación y las actualizaciones necesarias sobre los riesgos y políticas de seguridad de la información aplicables a su puesto.
 - Provisión de Recursos:** La gerencia debe proveer el tiempo, el presupuesto y las herramientas necesarias para que los empleados puedan realizar sus funciones de forma segura.
 -  **Proceso Disciplinario Activo:** La dirección debe implementar y dar soporte a un proceso formal para tomar medidas disciplinarias cuando se detecte que un empleado ha violado las políticas de seguridad de manera intencional o negligente.



Cláusula 5: Controles organizacionales

Control 5.4 Responsabilidades de la dirección

- **Otra Información:** El propósito de fondo de este control es fomentar una cultura donde la seguridad de la información no sea vista como una imposición del departamento de TI, sino como una práctica de negocio natural respaldada por los líderes de la empresa.

💡 Para un auditor, las firmas en las políticas no son suficientes para demostrar que la gerencia cumple con este control. En la práctica, te sugiero aterrizar las "responsabilidades de la dirección" de la siguiente forma:

-El líder es el dueño del riesgo, no TI: Si el gerente de Recursos Humanos permite que sus coordinadores compartan contraseñas porque "así trabajan más rápido", la responsabilidad del riesgo es del gerente de RH, no del CISO. Asegúrate de que los gerentes de área entiendan que ellos rinden cuentas (tienen accountability) por los incidentes que ocurran en sus propios departamentos debido a malas prácticas.

-Evita el favoritismo en las excepciones: Un error común en las empresas es que las políticas aplican para todos, excepto para los directores porque "están muy ocupados". Si permites que el Director General use una contraseña débil o evite el doble factor de autenticación (MFA), estás destruyendo este control. La dirección debe ser la más estricta en cumplir.

-Vincula la seguridad a las evaluaciones de desempeño: La forma más efectiva de que los jefes y gerentes exigen seguridad a sus equipos es cuando a ellos mismos los evalúan por eso. Añade un indicador clave (KPI) a las evaluaciones anuales de los gerentes, por ejemplo: "Porcentaje de su equipo que completó el curso anual de ciberseguridad antes de la fecha límite". Verás cómo se vuelven los principales impulsores del cumplimiento.



Cláusula 5: Controles organizacionales

Control 5.5 Contacto con las autoridades

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

- **Control:** La organización debe establecer y mantener contactos con las autoridades pertinentes.
- **Resumen de las Directrices de Implementación:** Este control se enfoca en la preparación operativa para reaccionar ante incidentes graves, asegurando que la empresa sepa exactamente a quién acudir cuando se vulnera la ley o la seguridad nacional/infraestructura crítica:
 - Identificación de Autoridades:** La organización debe mostrar claramente qué autoridades son relevantes según su ubicación geográfica y su sector empresarial. Esto incluye policía cibernética, agencias de protección de datos (como el INAI en México o la AEPD en España), reguladores financieros, servicios de emergencia y equipos de respuesta a incidentes nacionales (CERT/CSIRT).
 - Definición de Canales de Comunicación:** Se deben establecer procedimientos internos que especifiquen cuándo y cómo se debe contactar a estas autoridades. Esto evita que personal no autorizado filtre información confidencial o realice denuncias de forma incorrecta.
 - Tiempos de Respuesta y Notificación:** El control exige considerar los plazos legales obligatorios.
 - Reducción del Impacto:** Mantener estos lazos de forma proactiva permite que durante un ataque de Ransomware o una denegación de servicio (DDoS) la transferencia de evidencia forense y la solicitud de apoyo técnico institucional sean fluidas, acelerando la contención del daño.



Cláusula 5: Controles organizacionales

Control 5.5 Contacto con las autoridades

- Otra Información

Protección de Datos Personales: El contacto con las autoridades debe balancearse con las políticas de privacidad. Al reportar un incidente, se debe cuidar qué información confidencial de clientes o empleados se comparte, asegurando cumplir con los marcos legales locales para no incurrir en otra infracción

💡 Tener este control aprobado no consiste en poner en un documento el teléfono de emergencias de tu país. En el momento de un ataque de ciberseguridad real, el pánico reina y necesitas un directorio de acción inmediata. Te recomiendo lo siguiente:

-Crea una cartilla de contactos de "Pánico" actualizada: Construye una tabla específica dentro de tu Plan de Respuesta a Incidentes (IRP) que incluya: Nombre de la institución, nombre del contacto directo (si lo hay), teléfono de emergencias 24/7, correo electrónico de reporte y, crucialmente, el motivo por el cual los llamarías. Revisa este directorio cada 6 meses; las personas en las instituciones públicas cambian frecuentemente.

-Define la jerarquía de quién levanta el teléfono: No permitas que cualquier analista de TI llame a las autoridades o a la policía cibernética tras detectar una anomalía. Establece un flujo claro: el analista reporta al CISO, el CISO evalúa junto al área Legal y un portavoz autorizado (usualmente el Director Legal o el Oficial de Privacidad) realiza la notificación oficial.

-Haz simulacros de notificación (Tabletop Exercises): En tus ejercicios anuales de continuidad de negocio, simula que sufrieron una brecha de datos personales masiva. Haz que el equipo legal redacte el borrador de notificación para la autoridad de protección de datos bajo presión de tiempo. Descubrir que no saben qué formato usar o a qué plataforma subir el reporte durante el simulacro les ahorrará multas millonarias en la vida real.



Cláusula 5: Controles organizacionales

Control 5.6 Contacto con grupos de interés especial

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

- **Control:** La organización debe establecer y mantener contactos con grupos de interés especial u otros foros especializados en seguridad de la información y asociaciones profesionales.
- **Resumen de las Directrices de Implementación:** A diferencia del control anterior (orientado a entidades gubernamentales y regulatorias), este control se enfoca en la colaboración con la comunidad de ciberseguridad para mantener a la organización actualizada y protegida de forma proactiva:
 - Participación en Foros y Asociaciones:** Las organizaciones deben unirse a grupos de la industria, asociaciones profesionales o consorcios de intercambio de información .
 - Intercambio de Inteligencia de Amenazas:** El contacto debe servir para recibir y cuando sea apropiado, compartir información sobre nuevas vulnerabilidades, tácticas de atacantes (TTPs), indicadores de compromiso (IoCs) y mejores prácticas de seguridad.
 - Actualización del Estado del Arte:** Mantener estos lazos permite a los profesionales de la organización conocer las tendencias tecnológicas antes de que se vuelvan obsoletas y entender cómo otras empresas resuelven los mismos retos de seguridad.
 - Garantías de Confidencialidad:** Al participar en estos grupos, se debe tener especial cuidado con la información que la organización comparte hacia el exterior. Se debe asegurar el uso de protocolos de manejo de información (como el Traffic Light Protocol - TLP) para no revelar datos sensibles o debilidades internas de la empresa.



Cláusula 5: Controles organizacionales

Control 5.6 Contacto con grupos de interés especial

- Otra Información

Apoyo Mutuo en Crisis: En caso de un incidente de seguridad a gran escala, pertenecer a estos grupos proporciona acceso a una red de expertos independientes y competidores que colaboran mutuamente para mitigar un ataque común.

💡 Para pasar la auditoría de este control, no basta con decir que el CISO sigue a cuentas de ciberseguridad en X (Twitter) o LinkedIn. Necesitas demostrar una estructura de colaboración formal. Te recomiendo lo siguiente:

-Institucionaliza las membresías: Asegúrate de que las membresías a grupos clave (como ISACA o foros locales de seguridad) estén pagadas por el presupuesto de la empresa y no por el bolsillo del empleado. Si el empleado se va, la organización pierde el contacto y el control falla.

-Implementa el Protocolo TLP (Traffic Light Protocol): Cuando tu equipo técnico comparta información sobre un ataque en foros especializados, edúcalos sobre el protocolo TLP (Red, Amber, Green, Clear). Esto garantiza que sepan qué datos se pueden airear públicamente y cuáles deben quedarse estrictamente dentro de la comunidad de confianza.

-Aprovecha los ISAC sectoriales: Si tu empresa pertenece a un sector regulado (Fintech, Salud, Energía), busca el Information Sharing and Analysis Center de tu industria. Recibir correos de alerta temprana de tu propio sector vale oro para bloquear ataques antes de que toquen tu red.

-Evidencia para el auditor: Al auditor ISO le encanta la evidencia tangible. Guarda constancias de asistencia a congresos de ciberseguridad, correos de hilos de discusión técnicos donde participa tu equipo, boletines de vulnerabilidades a los que la empresa esté suscrita, o los certificados de las membresías vigentes del personal técnico.



Cláusula 5: Controles organizacionales

Control 5.7 Inteligencia de Amenazas

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

- **Control:** La información relacionada con las amenazas a la seguridad de la información debe ser recopilada y analizada para producir inteligencia de amenazas.
- **Resumen de las Directrices de Implementación:** Este control exige que las organizaciones dejen de esperar a ser atacadas y comiencen a entender a sus adversarios. La norma establece que la inteligencia de amenazas debe estructurarse en tres niveles jerárquicos:
 - Estratégico (Alto Nivel):** Información sobre el panorama global de amenazas, motivaciones de los atacantes (ej. geopolíticas, económicas) y tendencias tecnológicas. Sirve para que la dirección tome decisiones presupuestarias y de estrategia a largo plazo.
 - Táctico (Procesos y Técnicas):** Información sobre las metodologías, herramientas y tácticas de los atacantes (TTPs - Tactics, Techniques, and Procedures). Ayuda a los administradores a entender cómo operan los atacantes (por ejemplo, mediante el marco MITRE ATT&CK).
 - Operacional (Técnico e Inmediato):** Datos técnicos específicos sobre ataques en curso, como Indicadores de Compromiso (IoCs) que incluyen direcciones IP maliciosas, hashes de malware o dominios de phishing. Se inyecta directamente en los sistemas de defensa.



Cláusula 5: Controles organizacionales

Control 5.7 Inteligencia de Amenazas

- **El Proceso de Inteligencia:** La organización debe establecer un proceso que incluya:
 - Recopilación:** Fuentes internas (logs, incidentes previos) y externas (proveedores de ciberseguridad, agencias gubernamentales, foros del control 5.6).
 - Análisis:** Procesar los datos crudos para evaluar su relevancia, confiabilidad y contexto de negocio (saber si la amenaza realmente afecta a la tecnología que usa la empresa).
 - Acción:** Compartir los hallazgos con las partes interesadas y configurar los sistemas para bloquear o detectar proactivamente la amenaza identificada.
- **Otra Información:**
 - Automatización y Formatos Estándar:** Para que la inteligencia operacional funcione, se recomienda el uso de formatos abiertos de intercambio de datos como STIX (Structured Threat Information eXpression) y protocolos de transporte como TAXII (Trusted Automated eXchange of Intelligence Information), lo que permite que las herramientas tecnológicas "hablen" entre sí sin intervención humana constante.



Cláusula 5: Controles organizacionales

Control 5.7 Inteligencia de Amenazas

💡 La "Inteligencia de Amenazas" suena a ciencia ficción o a presupuesto millonario para contratar agencias de espionaje, pero en el mundo real puede implementarse de forma muy práctica. Te recomiendo lo siguiente:

-Implementa un ciclo de vida claro: Asegúrate de que el flujo de información esté documentado para el auditor. Una estructura básica e intuitiva para defender tu control es la del Ciclo de Inteligencia de Amenazas.

-Empieza gratis y automatizado: Si no tienes presupuesto para una plataforma comercial de Threat Intel (TIP), utiliza herramientas de código abierto como MISP (Malware Information Sharing Platform).

-Muestra evidencia de "Acción" al auditor: Al auditor no le interesa ver carpetas con reportes de PDF firmados sobre las nuevas tácticas de los hackers rusos. Lo que quiere ver es el impacto real. Muéstrale un caso como este: "El 14 de marzo recibimos un reporte táctico sobre un nuevo método de phishing automatizado (Inteligencia); el 15 de marzo creamos una regla en nuestro filtro de correo para bloquear ese patrón (Acción); el 16 de marzo el sistema bloqueó 40 intentos de entrada utilizando esa regla (Resultado)". Eso es cumplimiento perfecto del control 5.7.



Cláusula 5: Controles organizacionales

Control 5.8 Seguridad de la información en la gestión de proyectos

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

- **Control:** La seguridad de la información debe integrarse en la gestión de proyectos.
- **Resumen de las Directrices de Implementación:** Este control exige que la seguridad de la información no sea un agregado de última hora, sino un componente central desde la concepción de cualquier iniciativa (seguridad por diseño). Independientemente de si la organización utiliza metodologías tradicionales (Cascada) o metodologías ágiles (Scrum, DevOps), **los objetivos de seguridad deben estar integrados en todo el ciclo de vida del proyecto.**

Al inicio de cada proyecto se debe realizar un análisis de riesgos temprano para identificar amenazas específicas y definir los requisitos de seguridad correspondientes, tales como el cifrado de datos o la **gestión de accesos**. Asimismo, se deben establecer revisiones de calidad obligatorias (Gate Reviews) para condicionar el avance del proyecto al cumplimiento de hitos de seguridad, asegurando que las responsabilidades en la materia queden claramente asignadas entre los gerentes de proyecto, los desarrolladores y los especialistas en seguridad.



Cláusula 5: Controles organizacionales

Control 5.8 Seguridad de la información en la gestión de proyectos

- Otra Información:

Costo-Eficiencia: Integrar seguridad desde la fase de diseño es más económico y eficiente que corregir vulnerabilidades en producción.

💡 **Implementación Estratégica:** Para evitar ser un obstáculo a la innovación:

- Colabora** con la PMO para automatizar requisitos mediante plantillas o listas de verificación.

Integra controles de seguridad en la "Definición de Terminado" (Definition of Done) para equipos ágiles/Scrum.

- Participa** desde el inicio del proyecto en lugar de realizar auditorías de último momento.

- Ante lanzamientos con controles pendientes, documenta formalmente el riesgo residual y obtén la aceptación de la dirección. Esto demuestra madurez en la gestión de riesgos ante auditorías ISO.



Cláusula 5: Controles organizacionales

Control 5.9 Inventario de información y otros activos asociados

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

- **Control:** Se debe identificar la información y otros activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- **Resumen de las Directrices de Implementación:** Este control establece que una organización no puede proteger lo que no sabe que tiene. El inventario es la base para la gestión de riesgos y la asignación de controles:
 - Alcance del Inventario:** El inventario no solo debe incluir hardware. Debe registrar de manera clara:
 - Información:** Bases de datos, archivos físicos, propiedad intelectual, datos de clientes.
 - Activos de Software:** Aplicaciones, sistemas operativos, herramientas de desarrollo.
 - Activos Físicos:** Servidores, laptops, dispositivos móviles, medios de almacenamiento de respaldo.
 - Servicios:** Servicios en la nube (SaaS, PaaS, IaaS), servicios de red, utilidades (energía, aire acondicionado).
 - Propiedad del Activo (Asset Owner):** Cada activo listado en el inventario debe tener un "propietario" asignado (un rol o departamento, no necesariamente un individuo específico). El propietario es el responsable de definir cómo se clasifica y protege ese activo.
 - Ciclo de Vida:** El inventario debe mantenerse actualizado de forma continua. Deben existir procesos para registrar nuevos activos, modificar los existentes y dar de baja (destruir o borrar de forma segura) los activos obsoletos.



Cláusula 5: Controles organizacionales

Control 5.9 Inventario de información y otros activos asociados

- Otra Información

Relación con Gestión de Configuración: Para organizaciones grandes o con infraestructura compleja, este control se alinea estrechamente con la Gestión de la Configuración (CMDB). El valor del inventario aumenta drásticamente cuando se documentan las interconexiones (por ejemplo, saber qué base de datos de información confidencial corre sobre qué servidor físico específico). 🚫 **¡Cuidado! LA CMDB no debe considerarse un Inventario, el alcance y su funcionalidad son diferentes.**

💡 **Validar concepto Servicios en Alcance:** Los controles (como los que hemos venido revisando: 5.1, 5.7, 5.9, etc.) no se implementan por "amor al arte" o por cumplir la norma a ciegas. Los controles existen única y exclusivamente para mitigar los riesgos que amenazan al servicio dentro del alcance.

💡 **El peligro del "Excel eterno":** El error más común al implementar este control es crear una hoja de Excel masiva, llenarla una vez para la auditoría y dejar que se llene de polvo digital. En un par de meses estará obsoleta. **Automatiza lo que puedas.**

💡 **Define el nivel de granularidad** (No cuentes mouse por mouse): El inventario debe ser útil para gestionar riesgos de seguridad. Asociado al concepto **Valor**.

💡 **El "Dueño del Activo" no es el Administrador de TI (Responsable del activo):** Es muy común asignar al Director de TI como dueño de todos los servidores y bases de datos de la empresa. Esto es un error de concepto. El dueño de la base de datos de nómina es el Gerente de Recursos Humanos; TI solo provee la infraestructura para guardarla (custodio). **El dueño de negocio es quien debe decidir quién tiene permiso de ver la información y qué tan crítica es para la operación si llega a borrarse.**



Cláusula 5: Controles organizacionales

Control 5.10 Uso aceptable de la información y otros activos asociados

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

- **Control:**

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y otros activos asociados con la información y las instalaciones de procesamiento de información.
- Resumen de las Directrices de Implementación:Este control define las "reglas de conducta" y las expectativas de la organización sobre cómo los empleados y contratistas deben interactuar con los recursos tecnológicos e informáticos:
 - Desarrollo de Reglas Claras:** La organización debe crear una política o conjunto de reglas que dejen claro qué está permitido y qué está prohibido hacer con los activos (laptops, internet, correo electrónico, sistemas, etc.).
 - Compromiso del Personal:** Todo el personal que tenga acceso a los activos debe conocer, comprender y firmar de conformidad estas reglas de uso aceptable antes de que se les otorguen privilegios de acceso.
 - Uso Personal de los Activos:** La norma indica que la **política** debe especificar si se permite el uso personal de los activos de la empresa (por ejemplo, revisar redes sociales o correo personal desde la laptop corporativa) y de ser así, bajo qué condiciones o límites.
 - Monitoreo y Privacidad:** Las reglas deben informar claramente a los usuarios si la organización realiza monitoreo de sus actividades (revisión de tráfico de internet, auditoría de correos corporativos), respetando siempre las leyes locales de privacidad laboral.



Cláusula 5: Controles organizacionales

Control 5.10 Uso aceptable de la información y otros activos asociados

- Otra Información

Terminación de la Responsabilidad: Las reglas de uso aceptable deben seguir vigentes o tener cláusulas de confidencialidad remanentes incluso si el empleado deja la organización, asegurando que los activos devueltos se manejen correctamente y no se extraiga información en el proceso de salida.

💡 En el contexto estricto de la norma ISO/IEC 27002:2022, quien define el uso aceptable de la información y de los activos asociados es el Propietario del Activo (Asset Owner), un rol que ya identificamos previamente en el Control 5.9.

Ejemplo: El Gerente de Finanzas (dueño del sistema de facturación) determina que ese activo solo puede ser usado por personal de su área y prohíbe estrictamente que se extraigan reportes en dispositivos USB. El área de Seguridad no inventa esa regla; el dueño del activo la define según la sensibilidad de su operación.



Cláusula 5: Controles organizacionales

Control 5.11 Devolución de activos

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

- **Control:** Todos los empleados y partes interesadas externas deben devolver todos los activos de la organización que estén en su poder al terminar su empleo, contrato o acuerdo.
- **Resumen de las Directrices de Implementación:** Este control se enfoca en el proceso de salida (offboarding) del personal o proveedores, asegurando que la organización recupere el control físico y lógico de sus recursos para evitar fugas de información:
 - Proceso de Devolución Formalizado:** La organización debe tener un procedimiento documentado que dicte cómo se deben entregar los activos cuando un contrato finaliza (ya sea por renuncia, despido o término de servicios con un proveedor).
 - Alcance de los Activos a Devolver:** No solo se limita a equipos físicos. El personal debe devolver o destruir de forma segura:
 - Equipo físico (laptops, teléfonos corporativos, tokens de seguridad, tarjetas de acceso).
 - Copias de información (respaldos en discos duros externos, documentos impresos confidenciales).
 - 🔑 **Credenciales, Uniformes** y accesos (se deben revocar las cuentas de software y accesos a la nube).
 - Propiedad Intelectual y Datos:** En casos donde el empleado haya utilizado dispositivos personales (BYOD) o cuentas personales autorizadas temporalmente, se debe verificar que toda la información propiedad de la empresa haya sido eliminada de dichos medios.
 - Firma de Conformidad:** Tanto la organización como el empleado que se retira deben firmar un documento donde conste que todos los activos listados en su inventario personal (visto en el control 5.9) han sido devueltos satisfactoriamente.



Cláusula 5: Controles organizacionales

Control 5.11 Devolución de activos

- Otra Información

Casos de Despido Hostil: Si la terminación de la relación laboral es conflictiva, las directrices de la norma sugieren que la revocación de accesos lógicos e informáticos ocurra antes de notificar oficialmente al empleado sobre su baja, previniendo así posibles actos de sabotaje, borrado de datos o robo de información de último minuto.

💡 Vincula el inventario personal al checklist de RH: El control 5.11 es imposible de cumplir si Recursos Humanos no sabe qué tiene el empleado en sus manos; **Automatiza el "apagón"** de cuentas: El eslabón más débil de este control son las cuentas en la nube (SaaS) como HubSpot, AWS o herramientas de diseño que no siempre están amarradas al Directorio Activo.

💡 **Lo que te pedirá el auditor:** El auditor le pedirá a Recursos Humanos una lista de las personas que dejaron la empresa en los últimos 3 meses. Luego, elegirá dos nombres y te pedirá: 1) La carta de entrega-recepción de activos firmada por el ex-empleado y por TI, y 2) La evidencia técnica (con fecha y hora) de que sus cuentas de correo y accesos fueron desactivados el mismo día de su salida. Si las fechas no coinciden, tendrás una observación en tu reporte.



Cláusula 5: Controles organizacionales

Control 5.12 Clasificación de la información

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

- **Control:** La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización basadas en la confidencialidad, la integridad, la disponibilidad y los requisitos de las partes interesadas pertinentes.
- **Resumen de las Directrices de Implementación:** Este control exige que la organización categorice su información en diferentes niveles para poder asignarle una protección proporcional a su valor, evitando gastar recursos excesivos en datos públicos o desproteger datos críticos:
 - Esquema de Clasificación:** Se debe definir un esquema claro con niveles de clasificación. Aunque el estándar más común en la industria se basa en la confidencialidad (ej. Pública, Interna, Confidencial, Secreta), la norma recuerda explícitamente que también se debe considerar el impacto en la integridad y la disponibilidad si esos datos se alteran o se pierden.
 - Criterios de Clasificación:** El esquema debe basarse en el valor de la información para el negocio y el daño potencial (financiero, legal, regulatorio o reputacional) que causaría una brecha de seguridad.
 - Responsabilidad del Dueño:** El **propietario del activo** (identificado bajo el control 5.9) es el **responsable** directo de determinar y asignar el nivel de clasificación a la información que genera o administra.
 - Alineación con Socios y Clientes:** El esquema debe considerar las necesidades de las partes interesadas (por ejemplo, si un cliente exige contractualmente que sus datos se manejen bajo etiquetas o restricciones específicas).
 - Revisión Periódica:** Las clasificaciones deben revisarse a intervalos planificados, ya que el nivel de sensibilidad de un documento puede disminuir con el tiempo (por ejemplo, un reporte financiero secreto deja de serlo una vez que se publica oficialmente).



Cláusula 5: Controles organizacionales

Control 5.12 Clasificación de la información

- Otra Información

Simplificación: La norma sugiere explícitamente mantener el esquema lo más simple posible. Tener demasiados niveles de clasificación (ej. más de 4 o 5) confunde al personal operativo, eleva los costos de gestión y suele provocar que el control falle en el día a día.

💡 **Crea una matriz de "Consecuencias de Impacto":** Para que tus empleados clasifiquen los documentos sin dudar, evita definiciones ambiguas como "Confidencial es lo que es importante". Sé ultra específico en tu política: "Confidencial es cualquier información cuya filtración genere una multa legal, la pérdida de un cliente o un impacto financiero directo superior a X cantidad de dinero". Si das parámetros medibles, la clasificación se vuelve un proceso objetivo.

💡 Por defecto, establece que todo es "**Uso Interno**": No satures a tu personal obligándolos a clasificar cada correo de felicitación de cumpleaños o minuta operativa. Decreta que toda la información creada dentro de la red corporativa se clasifica automáticamente como "Interna", y que el usuario solo debe cambiar la etiqueta activamente si el documento es "Público" (hacia el exterior) o "Confidencial/Restringido" (sensible). Esto reduce drásticamente la fatiga del usuario.

💡 Automatiza las etiquetas con **herramientas** de descubrimiento de datos: En el entorno tecnológico actual, dejar la clasificación a la buena voluntad del empleado es un riesgo enorme. Utiliza herramientas como Microsoft Purview o sistemas Data Loss Prevention (DLP).

💡 **Lo que el auditor te va a pedir en la práctica:** El auditor no se conformará con ver el documento de la política de clasificación redactado. Te pedirá que abras tu inventario de activos (5.9) y verificará que cada repositorio de información tenga asignada su clasificación correspondiente. Luego, elegirá un documento sensible al azar (por ejemplo, los contratos de tus proveedores) y te preguntará: "Este documento está marcado como Confidencial, ¿dónde están las reglas que especifican quién puede leerlo, cómo se transporta y cómo se destruye?", lo cual te conectará directamente con el siguiente control de la norma (el 5.13 Etiquetado de la información).



Cláusula 5: Controles organizacionales

Control 5.13 Etiquetado de la información

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

- **Control:** Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.
- **Resumen de las Directrices de Implementación:** El etiquetado es el mecanismo que permite a los usuarios y a los sistemas informáticos identificar de un vistazo el nivel de protección que requiere un activo:
 - Procedimientos de Etiquetado:** La organización debe establecer reglas claras sobre cómo se debe marcar la información. Esto incluye formatos físicos (sellos, portadas) y digitales (marcas de agua, metadatos, encabezados).
 - Alcance Total:** El etiquetado debe aplicarse a la información en todos sus formatos y estados: documentos de texto, correos electrónicos, hojas de cálculo, bases de datos, medios de almacenamiento físico (USB, cintas de respaldo) e incluso listados impresos.
 - Excepciones Justificadas:** La norma reconoce que en ocasiones el etiquetado es imposible o contraproducente (por ejemplo, etiquetar visualmente un archivo de sistema interno podría dar pistas a un atacante, o etiquetar metadatos en un sistema de legado que no lo soporta). Estas excepciones deben documentarse.
 - Manejo de Activos Etiquetados:** Los procedimientos deben definir las reglas de custodia para cada etiqueta. Por ejemplo, qué tipo de transporte requiere un archivo "Secreto" (mensajería cifrada) versus uno "Interno".



Cláusula 5: Controles organizacionales

Control 5.13 Etiquetado de la información

- **Otra Información:**

Metadatos y Automatización: El etiquetado digital moderno no se limita a escribir "Confidencial" en el pie de página. Consiste en incrustar metadatos ocultos en el archivo para que las herramientas de ciberseguridad (como firewalls, sistemas de correo o DLP) puedan leer la etiqueta automáticamente y aplicar reglas de bloqueo si el archivo intenta salir de la red.

💡 **Adopta el etiquetado invisible (Metadatos):** No confíes en que tus empleados se acuerden de escribir "CONFIDENCIAL" en letras rojas dentro de cada propuesta comercial. Utiliza herramientas que inserten etiquetas de metadatos en los archivos (como las etiquetas de confidencialidad de Office 365 / Google Workspace). Esto permite que, si un empleado intenta arrastrar ese documento a un USB o subirlo a su cuenta personal de Gmail, el sistema operativo o el navegador lean el metadato oculto y bloqueen la acción de inmediato.

💡 **Automatiza las marcas de agua en la impresión:** Si tu negocio maneja planos, contratos o información médica y es inevitable imprimir en papel, configura las impresoras corporativas para que añadan automáticamente una marca de agua diagonal con el nivel de clasificación y, de ser posible, el nombre del usuario que mandó a imprimir. Esto disuade drásticamente las fugas de información físicas.

💡 **Etiqueta los contenedores, no solo los archivos:** En bases de datos masivas o servidores de archivos, etiquetar registro por registro es técnicamente inviable. La mejor práctica es etiquetar el "contenedor". Si una base de datos aloja la información de tarjetas de crédito de tus clientes, etiqueta y clasifica todo el servidor de la base de datos como "Restringido/Confidencial" y aplica las reglas de protección a todo el entorno.

💡 **Lo que el auditor va a revisar:** El auditor te pedirá ver ejemplos reales de información etiquetada en diferentes formatos. Te pedirá que le muestres cómo se ve un correo electrónico confidencial saliendo de la empresa, cómo se etiqueta un archivo PDF sensible en tu repositorio en la nube y cómo marcas físicamente los discos duros externos o respaldos que guardas bajo llave. Asegúrate de que el formato de la etiqueta coincida exactamente con lo redactado en tu política.



Cláusula 5: Controles organizacionales

Control 5.14 Transferencia de información

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

- **Control:** Se deben establecer reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
- **Resumen de las Directrices de Implementación:** Este control busca mitigar los riesgos asociados con el intercambio de datos a través de cualquier canal (electrónico, físico o verbal). Las directrices clave incluyen:
 - Procedimientos de Transferencia Segura:** La organización debe contar con reglas claras sobre cómo enviar información. Esto incluye el uso de canales electrónicos seguros (protocolos cifrados como HTTPS, SFTP, correos encriptados) y métodos físicos resguardados.
 - Acuerdos de Transferencia (Acuerdos de Compartición de Datos / DSA):** Cuando se intercambia información con terceras partes (proveedores, socios, clientes), se deben firmar acuerdos formales que especifiquen las responsabilidades de seguridad, los niveles de cifrado requeridos y las consecuencias en caso de una brecha.
 - Protección del Mensaje y el Canal:** Se deben implementar controles para proteger la información en tránsito contra interceptaciones, copias ilegales, modificaciones o destrucción. El cifrado de extremo a extremo es la práctica estándar recomendada.
 - Trazabilidad y No Repudio:** Se deben mantener registros (logs) de las transferencias críticas, permitiendo saber con certeza quién envió qué archivo, a quién, y cuándo se recibió.
 - Uso de Herramientas Autorizadas:** Se debe prohibir explícitamente el uso de canales de transferencia no oficiales o inseguros (como servicios de mensajería comercial no controlados por la empresa) para fines corporativos



Cláusula 5: Controles organizacionales

Control 5.14 Transferencia de información

- Otra Información

Políticas de Escritorio Limpio y Pantalla Limpia (Ligado al Control 7.7): La transferencia de información también puede ocurrir de manera visual o verbal. Las directrices recuerdan la importancia de no dejar información clasificada a la vista de visitas o personas no autorizadas durante procesos de transferencia física.

💡 **Elimina las transferencias por "correo tradicional" para archivos sensibles:** El correo electrónico estándar no es un canal seguro para mover bases de datos o contratos confidenciales. Implementa una plataforma de MFT (Managed File Transfer) o soluciones en la nube corporativas donde el usuario envíe un enlace seguro y temporal con contraseña en lugar de adjuntar el archivo directamente.

💡 **Define reglas estrictas para el uso de herramientas de chat (Slack, Teams, WhatsApp):** Es muy común que los empleados utilicen los chats corporativos para pasarse contraseñas, tokens de API o bases de datos rápidas de clientes. Configura tus herramientas de comunicación interna para bloquear el envío de ciertos tipos de extensiones de archivos (como .csv o .sql) a través de chats generales y refuerza las políticas de borrado automático de mensajes antiguos.

💡 **Firmas de convenios de confidencialidad (NDA / DSA):** Trabaja con el equipo legal para que cualquier contrato con un nuevo cliente o proveedor incluya de forma obligatoria un anexo de transferencia segura de datos. Si el auditor te pregunta cómo aseguras la confidencialidad con un tercero, mostrarle la cláusula estándar firmada dentro del contrato comercial es la evidencia más sólida que puedes presentar.

💡 **La prueba de fuego del auditor:** El auditor te pedirá ver el flujo de salida de información. Podría pedirte: "Muéstrame cómo le envían la información contable al despacho de auditoría externa". Tendrás que demostrarle que se utiliza un canal cifrado, que existe un convenio de confidencialidad firmado con ese despacho, y mostrarle los registros del sistema (logs) que prueban que solo las personas autorizadas pueden descargar esos archivos.



Cláusula 5: Controles organizacionales

Control 5.15 Control de acceso

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

- **Control:** Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse de acuerdo con las necesidades operativas y de seguridad de la información del negocio.
- **Resumen de las Directrices de Implementación:** Este control exige que la organización determine quién, cómo y cuándo tiene permitido interactuar con sus recursos informáticos y físicos, limitando los privilegios al mínimo necesario:
 - Política de Control de Acceso:** La organización debe documentar reglas claras que gobiernen tanto el acceso lógico (sistemas, redes, software, archivos) como el acceso físico (oficinas, centros de datos).
 - Principio de Menor Privilegio:** A los usuarios (empleados, contratistas, sistemas automatizados) sólo se les deben otorgar los accesos estrictamente necesarios para desempeñar su función laboral. Tener privilegios "por si acaso" está prohibido.
 - Necesidad de Conocer (Need-to-Know):** El acceso a información específica debe otorgarse únicamente si el rol del usuario requiere interactuar con esos datos para cumplir con sus responsabilidades de negocio.
 - Ciclo de Vida del Acceso:** El control abarca todo el ciclo del usuario: la solicitud formal del acceso, la autorización por parte del dueño del activo, la asignación técnica, la revisión periódica y la revocación inmediata en caso de cambio de puesto o despido (ligado al control 5.11).
 - Seguridad de la Red y Sistemas:** Se deben establecer barreras lógicas (como firewalls, autenticación y listas de control de acceso) para segregar y proteger las redes internas según el nivel de sensibilidad del activo.



Cláusula 5: Controles organizacionales

Control 5.15 Control de acceso

- Otra Información

Alineación con el Negocio: Las reglas de control de acceso no deben basarse únicamente en criterios de TI; deben responder directamente a los requisitos operativos del negocio, las leyes de privacidad aplicables (como el manejo de datos personales) y los acuerdos contractuales con clientes.

💡 **Adopta un modelo RBAC (Role-Based Access Control):** Olvídate de asignar permisos usuario por usuario en tus carpetas compartidas o sistemas; esto se vuelve ingobernable en poco tiempo. Diseña perfiles de acceso basados en roles de puesto estandarizados (ej. "Analista de Contabilidad", "Coordinador de Soporte"). De este modo, cuando entre un empleado nuevo, solo le asignas el rol preconfigurado y hereda automáticamente los accesos justos, facilitando el cumplimiento del menor privilegio.

💡 **Implementa revisiones de acceso ("User Access Reviews") con calendario:** Al auditor no le basta con saber que asignas bien los accesos; quiere ver cómo limpias los sistemas. Programa revisiones trimestrales o semestrales obligatorias donde envíes a cada director de área la lista de personas que tienen acceso a sus sistemas para que firmen de conformidad que todos siguen necesitando esos permisos. Te sorprenderá cuántos accesos obsoletos de personas que cambiaron de departamento se eliminan con esta práctica.

Es muy común que cuando un empleado se va, TI borre su cuenta de correo, pero Recursos Humanos olvide retirar su tarjeta de acceso biométrico a las oficinas, o viceversa. Asegúrate de unificar el checklist de baja para que ambos mundos del control de acceso (físico y digital) se cancelen de forma simultánea.

💡 **Lo que el auditor va a pedir en la práctica:** El auditor de la ISO 27001 irá directamente a buscar incoherencias. Te pedirá tu listado de personal activo y lo cruzará contra la lista de usuarios administradores en tu Directorio Activo o ERP corporativo. Si encuentra una cuenta genérica tipo "Contabilidad1" o el usuario de una persona que ya no trabaja en la organización, el control estará reprobado. Diseña un proceso claro donde cada acceso concedido esté respaldado por un ticket de soporte o correo de autorización del dueño del sistema.



Cláusula 5: Controles organizacionales

Control 5.16 Gestión de la identidad

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

- **Control:** Se debe gestionar el ciclo de vida completo de las identidades de los usuarios, de los dispositivos y de los servicios.
- **Resumen de las Directrices de Implementación:** Este control exige establecer un proceso riguroso para asegurar que cada entidad (humana o automatizada) dentro de la red corporativa esté correctamente registrada, validada y asociada a una identidad única:
 - Ciclo de Vida de la Identidad:** La organización debe controlar todas las fases de una identidad informática: creación (provisión al ingresar a la empresa), mantenimiento (actualización por cambios de rol o puesto) y terminación (desprovisión o eliminación al salir de la organización).
 - Identidades Únicas:** Se debe garantizar que cada usuario tenga un identificador único (ID de usuario). Está explícitamente prohibido el uso de identidades compartidas o genéricas para actividades cotidianas, ya que destruyen la trazabilidad y la rendición de cuentas.
 - Entidades No Humanas:** El control no solo aplica a personas; también exige gestionar las identidades de dispositivos (laptops, servidores, celulares autorizados) y servicios/aplicaciones (cuentas de servicio, conexiones API, scripts automatizados).
 - Proceso de Verificación:** Antes de emitir o activar una identidad digital, se debe verificar la identidad del solicitante en el mundo real (por ejemplo, validación de documentos de identidad por parte de Recursos Humanos o firmas notariales en el caso de contratistas).
 - Identidades Temporales:** Se deben establecer controles estrictos y fechas de caducidad automática para cuentas de invitados, auditores externos o personal temporal.



Cláusula 5: Controles organizacionales

Control 5.16 Gestión de la identidad

- Otra Información

Cuentas Duplicadas y Residuos: Las directrices enfatizan la necesidad de implementar **revisiones periódicas** para detectar "identidades huérfanas" o cuentas duplicadas que un mismo usuario haya acumulado a lo largo del tiempo, ya que representan vectores de ataque críticos.

💡 **Vincula el ciclo de vida al Directorio Activo (Identity Provider):** No permitas que cada sistema de la empresa tenga su propia base de datos de usuarios aislada. Utiliza un proveedor de identidad centralizado (IdP) como Microsoft Entra ID (Azure AD), Okta o Google Workspace. Al unificar las identidades, cuando un empleado sea dado de baja en el sistema central de Recursos Humanos, su identidad digital completa se desactivará automáticamente en todos los servicios de la empresa de un solo golpe.

💡 **Establece una política estricta de "Cuentas de Servicio":** El talón de Aquiles de este control suelen ser los sistemas que se comunican entre sí (APIs). Los desarrolladores suelen crear cuentas llamadas "Usuario_Pruebas" o "Servicio_API" con contraseñas que nunca expiran. Trata a estas identidades automatizadas con el mismo rigor que a un humano: documéntalas en un registro técnico, asígnales un responsable (un dueño de sistema) y audita sus permisos periódicamente.

💡 **Prohíbe los usuarios compartidos (El clásico "Soporte" o "Admin"):** Si tres administradores de TI usan la cuenta genérica "Administrador" para configurar los servidores, y un día se borra una base de datos crítica, nunca sabrás quién fue. Si el uso de una cuenta genérica es técnicamente obligatorio por restricciones del software, implementa una solución de PAM (Privileged Access Management) que "recueste" la cuenta y obligue al administrador a identificarse con su usuario personal antes de otorgarle la contraseña temporal del usuario maestro.

💡 **Lo que el auditor va a revisar:** El auditor te pedirá el listado de usuarios de tus sistemas principales y buscará nombres que parezcan genéricos o IDs ambiguos (ej. "recepción", "invitado123"). Te pedirá la evidencia documental o el ticket de soporte de cómo se validó la identidad de la persona detrás de esa cuenta antes de crearla.



Cláusula 5: Controles organizacionales

Control 5.17 Información de Autenticación

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

Control: La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión formal, que incluya asesorar a los usuarios sobre el manejo correcto de la información de autenticación.

- **Resumen de las Directrices de Implementación:** Este control regula cómo se crea, distribuye, almacena y cambia la información utilizada para probar una **identidad** (contraseñas, códigos MFA, llaves criptográficas, certificados digitales o datos biométricos):
 - Proceso Formal de Asignación:** Cuando se genera una nueva cuenta, la credencial temporal inicial debe entregarse al usuario a través de un canal seguro y debe obligarse a su cambio inmediato en el primer inicio de sesión.
 - Educación al Usuario:** La organización debe capacitar explícitamente a su personal en buenas prácticas de credenciales, prohibiendo actividades como:
 - Compartir contraseñas con compañeros o supervisores o anotar contraseñas en notas físicas (Post-its) o archivos de texto sin cifrar.
 - Reutilizar contraseñas corporativas en servicios personales (redes sociales, tiendas en línea).
 - Sistemas de Autenticación Robustos:** Se deben implementar tecnologías que fuercen la complejidad de las credenciales, impidan el uso de palabras comunes y requieran Autenticación Multi-Factor (MFA) para accesos críticos o remotos.
 - Almacenamiento Seguro:** La información de autenticación nunca debe almacenarse en texto plano en las bases de datos; debe protegerse utilizando algoritmos de encriptación y funciones de hash robustas con sal (salted hash).



Cláusula 5: Controles organizacionales

Control 5.17 Información de Autenticación

- Otra Información

Cambiando el Paradigma: Las directrices actuales de la norma reflejan las tendencias modernas de ciberseguridad: en lugar de obligar a los usuarios a cambiar contraseñas cada 30 o 90 días de forma arbitraria (lo que suele llevar a contraseñas predecibles como Verano2026), **se prefiere mantener contraseñas largas (frases de contraseña) combinadas obligatoriamente con MFA y sistemas de monitoreo de inicio de sesión anómalos.**

💡 **Implementa un Gestor de Contraseñas Corporativo:** Exigirle a los empleados que memoricen 40 contraseñas complejas y diferentes para cada sistema de la empresa es una batalla perdida; terminarán anotándolas bajo el teclado. Provee una herramienta institucional como 1Password, Bitwarden o Keeper. Esto les permite generar credenciales aleatorias y ultra seguras para cada aplicación sin necesidad de recordarlas, mitigando el riesgo de reutilización de contraseñas.

💡 **MFA no es opcional, es el estándar obligatorio:** Una contraseña compleja ya no es suficiente en el panorama de amenazas actual. Activa la **autenticación multifactor (MFA)** en absolutamente todos los puntos de entrada lógicos de la empresa. Prioriza el uso de aplicaciones de autenticación (como Microsoft Authenticator o Google Authenticator) o llaves físicas (FIDO2) por encima de los mensajes SMS, los cuales son vulnerables a ataques de duplicación de SIM (SIM swapping).

💡 **Configura el bloqueo automático y umbrales de intento:** Protege tus sistemas contra ataques de fuerza bruta configurando bloqueos temporales de cuenta tras un número específico de intentos fallidos (por ejemplo, bloquear la cuenta por 15 minutos tras 5 intentos erróneos). Acompaña esto con alertas automáticas al equipo de seguridad si se detectan múltiples bloqueos simultáneos en la red.

💡 **Lo que el auditor va a revisar:** El auditor querrá comprobar que las reglas de la política se aplican a nivel técnico. Te pedirá que muestres la configuración de las políticas de contraseñas y MFA en tu Directorio Activo o proveedor de identidad centralizado. Si tu política en papel dice "Las contraseñas deben tener al menos 12 caracteres y requerir MFA", pero al configurar una cuenta nueva el sistema permite contraseñas de 6 dígitos



Cláusula 5: Controles organizacionales

Control 5.18 Derechos de acceso

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

- **Control:** Los derechos de acceso a la información y otros activos asociados deben ser otorgados, revisados, modificados y eliminados de acuerdo con la política y las reglas específicas del tema de la organización para el control de acceso.
- **Resumen de las Directrices de Implementación:** Este control regula la parte operativa del ciclo de vida de los permisos, asegurando que ningún usuario acumule privilegios que no le correspondan:
 - Proceso Formal de Autorización:** El otorgamiento o modificación de cualquier derecho de acceso debe requerir una solicitud formal y la aprobación explícita del propietario del activo o de la información (según lo definido en el control 5.10).
 - Asignación Basada en Roles:** Los derechos deben configurarse idealmente agrupando usuarios en roles funcionales (RBAC), evitando la asignación manual e individual de permisos, lo cual eleva el riesgo de errores.
 - Revisiones Periódicas de Accesos:** La organización debe realizar auditorías de acceso regulares. Los accesos a sistemas críticos o con privilegios elevados deben revisarse con mayor frecuencia (ej. mensualmente), mientras que los accesos generales pueden revisarse de forma semestral o anual.
 - Revocación y Modificación Inmediata:** Cuando un empleado cambia de puesto dentro de la empresa o finaliza su contrato (offboarding), sus derechos de acceso deben ser modificados o eliminados de forma inmediata para evitar el acceso residual o el "abuso de privilegios acumulados".



Cláusula 5: Controles organizacionales

Control 5.18 Derechos de acceso

- Otra Información

Cuentas de Proveedores y Terceros: Las directrices hacen hincapié en que los derechos de acceso otorgados a proveedores externos o contratistas deben estar estrictamente delimitados en tiempo y alcance, deshabilitándose automáticamente una vez concluido el servicio pactado.

💡 **Corta de raíz el "Privilege Creep" (Acumulación de privilegios):** El mayor peligro en este control ocurre cuando un empleado es promovido o cambia de área (por ejemplo, pasa de Atención a Clientes al área de Finanzas). Lo común es que TI le otorgue los accesos de Finanzas pero olvide quitarle los de Atención a Clientes. Establece como regla técnica que todo cambio de puesto implica un "reseteo" total de derechos de acceso, obligando al nuevo jefe a solicitar desde cero únicamente lo que el colaborador necesita para su nuevo rol.

💡 **Implementa la "Firma de Re-certificación de Accesos":** No dejes las revisiones de acceso como una tarea informal de TI. Genera reportes automáticos desde tus sistemas y envíaselos a los Directores de cada área con una plantilla que diga "Certifico que las siguientes personas bajo mi cargo siguen requiriendo acceso a esta información confidencial". Su firma digital en ese reporte es la evidencia que dejará al auditor ISO completamente satisfecho.

💡 **Automatiza las alertas de cuentas inactivas:** Configura tu Directorio Activo o Identity Provider para que deshabilite automáticamente cualquier cuenta de usuario o de servicio que no haya registrado inicios de sesión en los últimos 30 o 45 días. Una cuenta inactiva pero con derechos de acceso vigentes es el blanco perfecto para los atacantes que buscan una puerta de entrada silenciosa a la organización.

💡 **Lo que el auditor va a revisar en la práctica:** El auditor te pedirá una lista de los empleados que se mudaron de puesto o salieron de la empresa recientemente. Luego, te pedirá que entres a los sistemas principales (como el ERP, CRM o bases de datos) y demuestres que los permisos antiguos de esas personas fueron efectivamente eliminados o ajustados el día exacto de su movimiento laboral.



Cláusula 5: Controles organizacionales

Control 5.19 Seguridad de la Información en la relación con proveedores

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

- **Control:** Se deben establecer e implementar procesos y requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización
- **Resumen de las Directrices de Implementación:** Este control exige que la organización no asuma que sus proveedores son seguros por defecto, sino que implemente un ciclo de vida formal para evaluar y controlar los riesgos de terceros (Third-Party Risk Management):
 - Identificación de Proveedores con Acceso:** La organización debe listar a todos los proveedores (SaaS, soporte de TI, consultores, limpieza, hosting) que tengan acceso, almacenen o procesen información corporativa o infraestructura crítica.
 - Evaluación de Riesgos Previa (Due Diligence):** Antes de firmar un contrato, se debe evaluar la postura de seguridad del proveedor mediante cuestionarios, revisiones de certificaciones.
 - Requisitos en Contratos (Control 5.20 relacionado):** Los contratos deben incluir cláusulas explícitas sobre las obligaciones de seguridad, la gestión de incidentes del proveedor, el derecho a auditar y los acuerdos de nivel de servicio (SLA).
 - Control de Accesos y Conexiones:** Si el proveedor requiere la red interna, se deben implementar canales cifrados específicos que operen bajo el principio de menor privilegio.
 - Cadena de Suministro (Subcontratistas):** La organización debe exigir al proveedor que extienda y controle estos mismos requisitos de seguridad hacia sus propios subcontratistas si estos interactúan con los datos compartidos.



Cláusula 5: Controles organizacionales

Control 5.19 Seguridad de la Información en la relación con proveedores

- Otra Información

Enfoque Basado en Riesgo: No todos los proveedores representan el mismo peligro. Las directrices recomiendan clasificar a los proveedores por niveles de criticidad (ej. Nivel 1: Alto riesgo / Acceso a base de datos de clientes, hasta Nivel 3: Bajo riesgo / Proveedor de papelería) para aplicar controles proporcionales al impacto potencial.

💡 **Crea un cuestionario de seguridad estándar para compras (Procurement):** Trabaja de la mano con el departamento de compras para que ninguna área de la empresa pueda contratar un software en la nube (SaaS) o un servicio externo sin que el proveedor pase primero por el filtro de seguridad. Diseña un formulario ágil de 10 o 15 preguntas críticas (ej. "¿Cuentan con cifrado en tránsito y reposo?", "¿Soportan MFA?", "¿Tienen certificación ISO 27001 o SOC 2?"). Si el proveedor reprueba el filtro o no responde, el proceso de compra debe detenerse automáticamente.

💡 **Clasifica a tus proveedores en niveles (Tiers):** Evita el error de auditar con la misma intensidad a la empresa que te renta los servidores en la nube que al proveedor del agua para las oficinas. Crea tres categorías basadas en el tipo de acceso a la información y enfoca tus esfuerzos de revisión exhaustiva únicamente en el "Top 10" de proveedores ultra críticos cuya caída o hackeo paralizaría tu servicio en alcance del SGSI.

💡 **El peligro del acceso remoto "eterno":** Es muy común darle acceso a un consultor externo a través de una VPN corporativa o una cuenta de administrador y olvidar retirarlo cuando el proyecto termina. Implementa políticas técnicas donde las cuentas de proveedores se deshabiliten de forma automática cada 30 días, obligando al gestor interno del proveedor a solicitar la extensión del acceso justificando que el servicio sigue activo.

💡 **Lo que el auditor va a pedir en la práctica:** El auditor te pedirá tu lista de proveedores en alcance. Elegirá un proveedor de la nube o de desarrollo de software y te dirá: "Muéstrame la evaluación de riesgos que le hiciste a esta empresa antes de contratarla y la evidencia técnica de cómo restringes y monitoreas sus accesos a tu plataforma corporativa". Si le muestras tu matriz de evaluación y los contratos comerciales con las cláusulas de seguridad firmadas, habrás superado la prueba.



Cláusula 5: Controles organizacionales

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

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

- **Control:** Se deben establecer y **acordar** requisitos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.
- **Resumen de las Directrices de Implementación:** Este control exige que los acuerdos legales (contratos, convenios de nivel de servicio o NDAs) dejen por escrito y de forma explícita las obligaciones de ciberseguridad que el proveedor debe cumplir durante toda la relación comercial:
 - Formalización de Acuerdos:** No se permiten acuerdos verbales ni de "buena fe" cuando hay activos de información involucrados. Las reglas deben estar plasmadas en contratos firmados por ambas partes antes de otorgar cualquier acceso.
 - Elementos Clave del Acuerdo:** Las directrices de la norma señalan que, como mínimo, los acuerdos deben definir:
 - La clasificación de la información que el proveedor manejará y los controles específicos de protección (ej. cifrado obligatorio).
 - El derecho de la organización a realizar auditorías independientes o solicitar reportes de seguridad del proveedor.
 - La obligación del proveedor de reportar cualquier incidente de seguridad que afecte a los datos de la organización dentro de un plazo estricto (ej. 24 o 48 horas).
 - La gestión del ciclo de vida de los datos al terminar el contrato (devolución o destrucción segura de la información).
 - Componentes de Infraestructura y Cadena de Suministro:** Si el proveedor suministra hardware o software, el acuerdo debe exigir garantías contra la manipulación indebida, código malicioso (malware) o componentes falsificados en la cadena de suministro.



Cláusula 5: Controles organizacionales

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

- Otra Información

Uso de Acuerdos Estándar: 🚀 La norma reconoce que con grandes proveedores de infraestructura en la nube (como AWS, Microsoft o Google), la organización no tiene poder de negociación para modificar sus contratos globales. En estos escenarios, el control se cumple revisando minuciosamente los términos de servicio estándares y los acuerdos de procesamiento de datos (DPA) preestablecidos por el gigante tecnológico para asegurar que se alineen al riesgo aceptable de la empresa.

💡 Diseña un "Anexo de Seguridad de la Información" (Data Security Addendum - DSA): **No intentes redactar cláusulas de ciberseguridad complejas directamente sobre el cuerpo del contrato comercial** tradicional, ya que los abogados comerciales suelen suavizar los términos para cerrar la venta rápido. Crea un documento técnico anexo estandarizado y obligatorio que contenga tus requerimientos duros (MFA, cifrado AES-256, parches al día). Si compras o el área legal van a contratar a un tercero, solo tienen que adjuntar este documento maestro al contrato principal.

💡 **Establece penalizaciones claras por ocultar incidentes:** El mayor peligro con un proveedor externo no es solo que lo hackeen, sino que intente ocultarlo por semanas para cuidar su reputación. Asegúrate de incluir en tus contratos cláusulas de penalización financiera o rescisión inmediata del servicio si el proveedor no notifica formalmente a tu equipo de seguridad sobre una sospecha de brecha de datos dentro del límite de tiempo acordado.

💡 **Define el destino final de los datos en el contrato:** Es muy común finalizar la relación con un proveedor de software y asumir que ellos borrarán tus bases de datos por educación. Exige contractualmente que, al término del servicio, el proveedor deba entregarte un "Certificado de Destrucción Segura de Datos" emitido bajo estándares internacionales (como NIST SP 800-88).

💡 **Lo que el auditor va a pedir en la práctica:** El auditor irá directamente al departamento legal o de compras. Elegirá al azar dos contratos de proveedores críticos firmados en el último año y buscará las firmas de aceptación de las cláusulas de seguridad, confidencialidad y derecho a auditoría. Si el contrato comercial no menciona sobre la protección de la información ni seguridad, el control se considerará deficiente o no conforme.



Cláusula 5: Controles organizacionales

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

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

- **Control:** Se deben establecer e implementar procesos y requisitos de seguridad de la información para mitigar los riesgos asociados con la cadena de suministro de productos y servicios de tecnologías de la información y comunicación (TIC).
- **Resumen de las Directrices de Implementación:** Este control va un paso más allá de la simple relación con el proveedor directo (controles 5.19 y 5.20), enfocándose en la trazabilidad y la integridad de todo el camino que recorre el hardware, software o servicio de TI antes de llegar a la organización:
 - Trazabilidad de la Cadena de Suministro:** La organización debe exigir a sus proveedores principales que demuestren de dónde obtienen sus **componentes** (chips, código fuente, servidores) para asegurar que no hayan sido manipulados de manera maliciosa en el trayecto.
 - Protección contra Componentes Falsificados:** Se deben implementar controles para verificar la autenticidad del hardware y software adquirido, evitando la introducción de componentes clonados o falsificados que puedan contener vulnerabilidades ocultas o "puertas traseras" (backdoors).
 - Seguridad en el Desarrollo por Terceros:** Si se contrata el desarrollo de software externo, se debe exigir al proveedor que demuestre que sus programadores siguen prácticas de desarrollo seguro y que el código entregado está libre de malware conocido.
 - Monitoreo de la Cadena de Subcontratación:** Los acuerdos con los proveedores de TIC deben obligarlos a notificar si van a subcontratar partes críticas del servicio a terceras empresas, permitiendo a la organización evaluar el riesgo de esa subcadena.



Cláusula 5: Controles organizacionales

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

- Otra Información

Riesgo Geopolítico y de Disponibilidad: Las directrices actuales de la norma enfatizan la necesidad de evaluar los riesgos de concentración de proveedores (dependen de un solo fabricante o de una sola región geográfica) para evitar que conflictos internacionales, desastres o sanciones dejen a la organización sin parches de seguridad o soporte técnico crítico.

💡 **Cuidado con las dependencias de Software Libre (Open Source Dependency Check):** En el mundo del software moderno, el 90% de las aplicaciones usan librerías gratuitas de terceros. El riesgo no suele estar en tu proveedor, sino en las dependencias que ese proveedor introduce sin saberlo. Exige a tus desarrolladores o proveedores de software que utilicen herramientas de análisis de composición de software (SCA) como Dependency-Check u Owasp Dependency Track para auditar que los componentes externos que inyectan en tu red no tengan vulnerabilidades críticas conocidas.

💡 **Establece un protocolo de "Inspección de Recepción" para hardware:** Cuando compres servidores, firewalls o switches de red críticos para tu infraestructura en alcance del SGSI, no los conectes directamente a la red de producción apenas lleguen en la caja.

💡 **Diversifica tus proveedores clave:** Aplicando la gestión de riesgos de la cadena de suministro, nunca permitas que un solo proveedor tenga el monopolio absoluto de tu tecnología vital. Si utilizas un servicio en la nube principal, asegúrate de tener una alternativa o un respaldo técnico en una infraestructura diferente.

💡 **Lo que el auditor va a pedir en la práctica:** El auditor de la ISO 27001 buscará comprobar cómo controlas lo que te entregan. Te dirá: "Muéstrame cómo te aseguras de que el software que te desarrolló este proveedor externo no trae código malicioso escondido". Para responder con éxito, muéstrale los reportes del escaneo de vulnerabilidades que le exiges al proveedor adjuntar con cada entrega los términos del contrato donde el proveedor se hace legalmente responsable por la integridad del software entregado.



Cláusula 5: Controles organizacionales

Control 5.22 Seguimiento, revisión y gestión de cambios de servicio de proveedores

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

- **Control:** La organización debe monitorear, revisar y auditar periódicamente los niveles de entrega de servicios de los proveedores y gestionar los cambios en los servicios de los proveedores.
- **Resumen de las Directrices de Implementación:** Este control exige que la organización mantenga una vigilancia activa sobre el desempeño de sus proveedores y controle estrictamente sus procesos de cambio:
 - Monitoreo de Desempeño y SLAs:** Se debe verificar de forma regular que el proveedor cumpla con los Acuerdos de Nivel de Servicio (SLA).
 - Revisiones e Informes de Seguridad:** La organización debe solicitar y revisar periódicamente los reportes de seguridad del proveedor, incluyendo bitácoras de acceso, parches aplicados, resultados de sus pruebas de vulnerabilidades o incidentes reportados.
 - Auditorías a Proveedores:** Dependiendo del nivel de riesgo del tercero, se deben realizar auditorías directas o, en su defecto, solicitar certificaciones de auditoría independientes y actualizadas (como reportes SOC 2 Tipo II o certificados ISO 27001 vigentes).
 - Gestión de Cambios del Proveedor:** Cualquier cambio significativo en el servicio del proveedor debe ser evaluado:
 - Actualizaciones mayores o cambios en las aplicaciones del proveedor.
 - Migraciones de datos o cambios en la ubicación geográfica de los centros de datos (data centers).
 - Cambios en los subcontratistas que el proveedor utiliza para dar el servicio.
 - Modificaciones en las políticas de seguridad o términos de servicio del proveedor.



Cláusula 5: Controles organizacionales

Control 5.22 Seguimiento, revisión y gestión de cambios de servicio de proveedores

- Otra Información

Mejora Continua y Reajuste: Si el monitoreo revela que el proveedor no cumple con los estándares exigidos de manera sistemática, o si el perfil de riesgo de la organización cambia, las directrices de la norma recomiendan actualizar la evaluación de riesgos y renegociar los contratos o buscar proveedores alternativos.

💡 **Crea un proceso formal para recibir notificaciones de cambio:** Los proveedores grandes suelen avisar sobre cambios en sus plataformas mediante correos masivos que terminan en la bandeja de spam. Asegúrate de configurar una cuenta de correo institucional genérica y regístrala ante tus proveedores críticos. El equipo de seguridad debe revisar este buzón semanalmente para evaluar si los cambios programados por el tercero afectan tus sistemas o el cumplimiento del SGSI.

💡 **No te fíes solo del estatus del proveedor, monitorea de forma externa:** Muchas empresas han sufrido caídas porque el sistema de un tercero falló, pero la página de estatus del proveedor seguía marcando "Todo verde".

💡 **Gestiona el impacto de la soberanía de datos en las migraciones:** Si tu proveedor de software en la nube te notifica que cambiará sus servidores de región (por ejemplo, de servidores en la Unión Europea a servidores en Estados Unidos), no lo firmes a la ligera. Esto puede violar las leyes locales de protección de datos personales o los contratos que tú tienes firmados con tus propios clientes. Evalúa legalmente el impacto de la ubicación de los datos antes de aceptar el cambio de infraestructura del proveedor.

💡 **Lo que el auditor va a pedir en la práctica:** El auditor de la ISO 27001 te dirá: "Muéstrame la última vez que un proveedor crítico te notificó un cambio técnico y cómo evaluaste el riesgo para tu organización". Para cumplir a la perfección, muéstrale una minuta, un ticket de soporte o un correo donde el equipo de seguridad analizó la notificación de un proveedor (ej. una ventana de mantenimiento mayor de AWS o la actualización de versión de tu ERP) y autorizó o adaptó los controles internos para absorber ese cambio de forma segura.



Cláusula 5: Controles organizacionales

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

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

- **Control:** Los procesos para la adquisición, el uso, la gestión y la salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
- **Resumen de las Directrices de Implementación:** Este control exige tratar a la nube bajo un ciclo de vida completamente gobernado, reconociendo que los entornos virtuales presentan riesgos de configuración y soberanía de datos muy particulares:
 - Establecimiento de una Política de la Nube:** La organización debe definir con claridad qué tipos de nubes (públicas, privadas o híbridas) y qué proveedores específicos están autorizados para manejar los datos del negocio.
 - Modelo de Responsabilidad Compartida:** Se debe comprender y documentar exhaustivamente qué controles de seguridad le corresponden al proveedor de la nube (ej. la seguridad física del centro de datos) y cuáles son responsabilidad directa e ineludible de la organización (ej. parches de los sistemas operativos virtuales, cifrado de datos y gestión de los accesos).
 - Gestión de la Configuración y Endurecimiento (Hardening):** Se deben definir líneas base de configuración segura para los entornos de nube (como el bloqueo de puertos públicos innecesarios) y evitar que configuraciones erróneas expongan información a internet.
 - Estrategia de Salida (Exit Strategy):** Desde el momento de la contratación, se debe planificar cómo se recuperará la información, cómo se migrará a otro entorno o cómo se eliminará de forma segura si se decide rescindir el contrato con el proveedor, evitando el secuestro técnico de datos (vendor lock-in).



Cláusula 5: Controles organizacionales

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

- Otra Información

Normas de Apoyo: Para organizaciones con una infraestructura que dependa fuertemente de estos entornos, la norma sugiere apoyarse de manera complementaria en los estándares **ISO/IEC 27017** (guía de controles de seguridad para servicios en la nube) e **ISO/IEC 27018** (protección de datos personales en nubes públicas).

💡 **Documenta formalmente tu Matriz de Responsabilidad Compartida:** El error más grave es asumir que por el simple hecho de alojar tus sistemas en Amazon Web Services, Microsoft Azure o Google Cloud, tu infraestructura ya es 100% inmune. **El proveedor es responsable de la seguridad de la nube, pero tú eres responsable del acceso la nube.** Diseña una matriz clara donde especifiques quién gestiona los respaldos, quién parcha las máquinas virtuales y quién activa el doble factor de autenticación (MFA) para las cuentas de administración.

💡 **Implementa herramientas de CSPM (Cloud Security Posture Management):** La gran mayoría de las brechas de seguridad catastróficas en la nube no ocurren por ataques de hackers ultra avanzados, sino por descuidos humanos (como dejar un contenedor de almacenamiento S3 de AWS o un Blob de Azure configurado como "Público" por error).

💡 **Combate el "Shadow IT" (Tecnología en las sombras):** Es sumamente común que los departamentos de Marketing, Ventas o Recursos Humanos contraten herramientas SaaS de forma independiente con una tarjeta de crédito corporativa, sin avisar al equipo de seguridad de la información. Configura bloqueos o auditorías en tus redes mediante soluciones CASB (Cloud Access Security Broker) para detectar y regular el uso de aplicaciones en la nube que no han pasado por el proceso de evaluación de riesgos de la empresa.

💡 **La pregunta típica del auditor:** El auditor te pedirá la lista de tus nubes en producción y te lanzará una pregunta clave: "Si este proveedor de la nube quiebra mañana o decide bloquear tu cuenta por una disputa comercial, ¿cuál es tu plan para recuperar los datos y mantener la operación del negocio?". Tener redactada una estrategia de salida o contar con respaldos fuera de ese ecosistema de nube te garantizará una conformidad impecable en este control.



Cláusula 5: Controles organizacionales

Control 5.24 Planificación y preparación para la gestión de incidentes de S.I.

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

- **Control:** La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información mediante el establecimiento, mantenimiento y comunicación de una política de gestión de incidentes de seguridad de la información, procedimientos y funciones y responsabilidades asociadas.
- **Resumen de las Directrices de Implementación:** Este control exige que la organización desarrolle una estructura formal (personas, procesos y políticas) para reaccionar de manera ágil, ordenada y sistemática ante cualquier sospecha de brecha de seguridad:
 - Política de Incidentes:** Se debe documentar una política que defina claramente qué constituye un "evento" (una anomalía sospechosa) y qué es un "incidente" (un evento confirmado que daña al negocio).
 - Roles y Responsabilidades Claras:** Se debe conformar formalmente el CIRT / CSIRT (Cyber Incident Response Team). Las funciones deben estar asignadas de antemano: quién coordina la respuesta técnica, quién toma las decisiones de negocio (ej. apagar un servidor crítico) y quién se encarga de la comunicación legal o pública.
 - Procedimientos de Escalación y Reporte:** Deben existir canales conocidos por todos los empleados y proveedores para reportar eventos de seguridad de inmediato. El plan debe incluir criterios de priorización (gravedad del impacto) para saber cuándo notificar a la alta dirección o a las autoridades reguladoras.
 - Pruebas y Simulacros:** Un plan que no se prueba no sirve. Las directrices exigen que los planes de respuesta se pongan a prueba periódicamente mediante simulacros (tabletop exercises o ejercicios prácticos) para asegurar que el equipo sabe cómo reaccionar bajo presión.



Cláusula 5: Controles organizacionales

Control 5.24 Planificación y preparación para la gestión de incidentes de S.I.

- Otra Información

Contactos con Autoridades: La preparación incluye mantener un directorio actualizado de contactos externos clave que deban ser notificados o consultados durante un incidente, tales como equipos nacionales de respuesta a emergencias (CERTs), proveedores de internet, forenses digitales externos o agencias de protección de datos (ligado al control 5.6).

💡 **Define una matriz de severidad objetiva:** No permitas que la clasificación de un incidente dependa del pánico del momento. Diseña una tabla donde un incidente sea "Crítico", "Alto" o "Medio" según datos medibles del servicio en alcance: por ejemplo, "Severidad Crítica = El sistema principal de facturación está caído por más de 30 minutos o hay evidencia de exfiltración de datos de clientes".

💡 **No dejes la comunicación en manos de TI:** Durante un incidente de ransomware o fuga de datos, el equipo de TI debe estar 100% enfocado en contener la amenaza. El plan de incidentes debe incluir obligatoriamente un rol de "**Comunicación** y Relaciones Públicas" y un filtro "Legal" que controlen la información que sale de la empresa, evitando declaraciones que empeoren la situación o generen multas.

💡 **La evidencia para el auditor:** Cuando el auditor revise el control 5.24, no solo querrá leer tu manual de gestión de incidentes. Te pedirá: 1) El acta de conformación oficial del comité de incidentes con nombres y puestos vigentes, y 2) La evidencia de que realizaste un simulacro (minutas, fotos de la sesión, el escenario evaluado y la lista de lecciones aprendidas). Mostrar que estás preparado proactivamente cerrará el control con una calificación excelente.



Cláusula 5: Controles organizacionales

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

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

- **Control:** La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.
- **Resumen de las Directrices de Implementación:** Este control regula el punto de transición crítico entre una simple sospecha (un evento) y una crisis confirmada (un incidente), asegurando que se activen los recursos correctos de manera oportuna:
 - Mecanismo de Clasificación:** La organización debe contar con un proceso claro para analizar los eventos reportados (ya sea por un usuario, un sistema de monitoreo automático o un proveedor) y compararlos con criterios preestablecidos.
 - Separación de Conceptos:**
 - Evento:** Una ocurrencia identificada en un sistema, servicio o red que indica una posible brecha de la política (ej. un usuario fallando su contraseña 5 veces o un pico inusual de tráfico).
 - Incidente:** Un evento o una serie de eventos no deseados que tienen una probabilidad significativa de comprometer las operaciones del negocio o la seguridad de los datos.
 - Responsable de la Decisión:** Debe existir un rol claramente asignado (generalmente el líder del CIRT, el CISO o un analista de seguridad de nivel superior) con la autoridad técnica para declarar formalmente un "Incidente de Seguridad".
 - Registro de Decisiones:** Tanto si el evento se descarta por ser una falsa alarma (falso positivo) como si se escala a incidente, el análisis y la justificación de la decisión deben quedar registrados de forma auditable.



Cláusula 5: Controles organizacionales

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

- Otra Información

Uso de Inteligencia de Amenazas (Ligado al Control 5.7): Para tomar decisiones rápidas y acertadas en la fase de evaluación, el equipo encargado debe apoyarse en datos actualizados de ciberseguridad para identificar si el evento detectado corresponde a un patrón de ataque activo en el mercado.

💡 **Reduce los falsos positivos automatizando el triaje inicial:** El equipo de seguridad puede sufrir "fatiga de alertas" si tiene que evaluar manualmente cada anomalía. Implementa reglas de correlación en tu SIEM o herramientas de monitoreo.

💡 **Crea un "Playbook" de preguntas rápidas para el decisor:** Para que la persona encargada no dude al declarar un incidente, proveerla de una guía rápida con tres preguntas de negocio: 1) ¿Hay datos confidenciales del alcance en riesgo de haber sido expuestos? 2) ¿El servicio core del negocio está interrumpido? 3) ¿Afecta a requisitos regulatorios o legales? Si alguna respuesta es afirmativa, no se analiza más se declara el incidente y se activa el plan de respuesta (Control 5.24).

💡 **Documenta los "Falsos Positivos" con rigor:** Cuando un evento parezca un ataque pero resulte ser una acción legítima (por ejemplo, un desarrollador ejecutando una prueba autorizada a medianoche), **no borres la alerta**. Regístrala en tu sistema de tickets y ciérrala bajo la etiqueta "Falso Positivo - Actividad Autorizada". Esto le demuestra al auditor que tu sistema sí detecta anomalías y que tu equipo ejerce un control analítico real sobre lo que ocurre en la red.

💡 **Lo que el auditor va a pedir en la práctica:** El auditor de la ISO 27001 te pedirá ver la bitácora histórica de eventos de seguridad de tus sistemas. Elegirá una alerta de nivel alto del mes pasado y te preguntará: "¿Quién revisó esta alerta, cuánto tiempo tardaron en evaluarla y bajo qué criterios decidieron que no era un incidente real?". Si le muestras el ticket de seguimiento cerrado con la justificación técnica de la evaluación, el control estará perfectamente defendido.



Cláusula 5: Controles organizacionales

Control 5.26 Respuesta a incidentes de seguridad de la información

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

- **Control:** Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados y se deben registrar las acciones de respuesta.
- **Resumen de las Directrices de Implementación:** Este control exige que la respuesta a un ataque o falla no sea improvisada, sino que siga una coreografía técnica y operativa previamente establecida para mitigar el impacto:
 - Ejecución de Procedimientos de Respuesta:** El equipo de respuesta a incidentes (CIRT) debe activar los protocolos específicos para el tipo de amenaza detectada (ej. procedimiento para ransomware, procedimiento para fuga de datos, procedimiento para denegación de servicio).
 - Contención, Erradicación y Recuperación:** Las acciones deben seguir un orden lógico e inmediato:
 - Contención:** Detener el avance del ataque para que no afecte a más sistemas (ej. aislar una computadora infectada de la red).
 - Erradicación:** Eliminar la causa raíz de la amenaza dentro de los sistemas (ej. borrar el malware o cerrar la cuenta comprometida).
 - Recuperación:** Restaurar los servicios afectados a su estado normal de operación.
 - Registro Exhaustivo (Bitácora):** Cada paso tomado durante la crisis debe quedar registrado con fecha, hora y responsable. Esto incluye llamadas telefónicas, comandos ejecutados en servidores, cambios de contraseñas o desconexión de equipos.
 - Notificación a Partes Interesadas:** El procedimiento debe dictar cuándo y cómo informar a entidades internas (alta dirección) y externas (clientes afectados, reguladores gubernamentales o socios de negocio) conforme a las leyes vigentes y los contratos (ligado al control 5.20).



Cláusula 5: Controles organizacionales

Control 5.26 Respuesta a incidentes de seguridad de la información

- Otra Información

Preservación de Evidencia (Ligado al Control 5.28): Durante la fase de respuesta y contención, el equipo técnico debe tener extremo cuidado de no alterar o destruir evidencia digital que pueda ser necesaria posteriormente para análisis forenses o procesos legales.

💡 Crea guías técnicas de una o dos páginas (Playbooks) para los escenarios más probables de tu servicio en alcance. El equipo de soporte debe saber qué cable desconectar o qué comando ejecutar si detectan un Ransomware en progreso, sin tener que esperar al CISO.

💡 **Establece un canal de comunicación alternativo de emergencia:** Durante un incidente grave, tu correo corporativo y tus chats internos de Teams o Slack podrían estar comprometidos o bajo control del atacante. Ten preparado un canal de comunicación alternativo y seguro fuera de la red corporativa para coordinar las acciones del comité de crisis sin que el atacante "escuche" la estrategia de mitigación.

💡 **Usa sistemas de tickets automáticos para la bitácora:** No pretendas que los ingenieros anoten lo que hacen en un bloc de notas mientras intentan salvar los servidores. Centraliza la respuesta en un ticket de seguridad y acostumbra al equipo a documentar ahí cada acción relevante de manera cronológica. Esa bitácora centralizada te ahorrará semanas de trabajo al momento de reconstruir los hechos y será la pieza central que valide tu control ante cualquier escrutinio.

💡 **Lo que el auditor va a pedir en la práctica:** El auditor te pedirá evidencia del último incidente real ocurrido en la organización. Querrá ver el ticket o expediente completo del caso. Revisará minuciosamente la línea del tiempo: "El incidente se declaró a las 10:00 AM, ¿a qué hora se contuvo?, ¿quién autorizó apagar el servidor?, ¿dónde está el registro de que los respaldos utilizados para restaurar estaban limpios?".



Cláusula 5: Controles organizacionales

Control 5.27 Aprendizaje de los incidentes de seguridad de la información

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

- **Control:** El conocimiento adquirido de los incidentes de seguridad de la información se debe utilizar para fortalecer y mejorar los controles de seguridad de la información.
- **Resumen de las Directrices de Implementación:** Este control exige que los incidentes no se archiven y olviden una vez solucionados. La organización debe implementar un proceso formal de "Lecciones Aprendidas" para cerrar el ciclo de mejora continua (Plan-Do-Check-Act):
 - Reunión Post-Incidente:** Tras el cierre de un incidente significativo, se debe convocar a una revisión formal con las partes clave involucradas para analizar qué sucedió y cómo se manejó.
 - Análisis de Causa Raíz (RCA):** Se debe identificar de manera exacta el factor origen que permitió el incidente.
 - Evaluación del Desempeño:** El equipo debe evaluar la efectividad de la respuesta ¿Los sistemas de monitoreo detectaron el ataque a tiempo?, ¿Los "Playbooks" funcionaron?, ¿El personal sabía qué hacer?
 - Implementación de Acciones Correctivas:** El resultado del análisis debe traducirse en un plan de acción con responsables y fechas límites para modificar políticas, reforzar configuraciones tecnológicas o capacitar al personal.
 - Actualización del Inventario de Riesgos:** El incidente es evidencia del mundo real de que una amenaza se materializó. Por lo tanto, la matriz de riesgos del SGSI debe actualizarse para reflejar esta nueva realidad.



Cláusula 5: Controles organizacionales

Control 5.27 Aprendizaje de los incidentes de seguridad de la información

- Otra Información

Compartir Información (Ligado al Control 5.7): Las directrices sugieren que, cuando sea apropiado y seguro, las lecciones aprendidas de un ataque se compartan con comunidades de ciberseguridad externas o ISACs (Information Sharing and Analysis Centers) para ayudar a proteger a otras organizaciones del sector.

💡 **Institucionaliza la reunión de "Post-Mortem":** No busques culpables, busca soluciones. Programa la sesión de lecciones aprendidas en un ambiente constructivo dentro de las primeras 72 horas posteriores al cierre del incidente, cuando los detalles técnicos aún están frescos en la mente de los ingenieros. Utiliza metodologías sencillas como los "5 Porqués" para excavar más allá de la superficie y encontrar la verdadera debilidad organizativa.

💡 **Genera un Reporte de Lecciones Aprendidas (LAL):** Documenta los hallazgos en un formato estandarizado que contenga de forma estricta: 1) Resumen del impacto, 2) Línea de tiempo del ataque, 3) Causa raíz identificada y 4) Tabla de compromisos de mejora. Este documento debe ser firmado por el CISO y el dueño del servicio afectado para garantizar el presupuesto y el apoyo en los cambios técnicos que se requieran.

💡 **Vincula las fallas a tu plan de concientización:** Si la causa raíz del incidente fue que un usuario de finanzas cayó en un ataque de phishing sofisticado y entregó sus credenciales, no te limites a resetear su contraseña. Toma ese caso de estudio (anonimizando el nombre del empleado para evitar el acoso laboral), adáptalo y utilízalo como ejemplo real en la siguiente campaña de capacitación en seguridad para toda la empresa. Nada educa mejor que los ejemplos de la vida real de la propia organización.

💡 **Lo que el auditor va a pedir en la práctica:** De la lista de incidentes que le mostraste en el control anterior (5.26), el auditor elegirá el caso más grave y te dirá: "Muéstrame el reporte de lecciones aprendidas de este ataque y el seguimiento a las acciones correctivas que determinaron".



Cláusula 5: Controles organizacionales

Control 5.28 Recopilación de evidencia

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

- **Control:** La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia digital relacionada con incidentes de seguridad de la información.
- **Resumen de las Directrices de Implementación:** Este control busca asegurar que las pruebas de un ataque informático (archivos de registro, imágenes de disco duro, volcados de memoria) se manejen con rigor científico y legal. Si la evidencia se altera, no servirá para auditorías internas, reclamaciones de seguros ni procesos judiciales:
 - Cadena de Custodia:** Se debe garantizar un registro ininterrumpido que demuestre quién tuvo acceso a la evidencia física o digital desde el momento en que se recolectó hasta su presentación final.
 - Preservación de la Integridad:** La regla de oro es nunca trabajar sobre el activo original. Se debe realizar una copia bit a bit (imagen forense) del medio de almacenamiento afectado y validar su integridad utilizando algoritmos de hash (como SHA-256).
 - Orden de Volatilidad:** Los analistas deben recolectar la información empezando por los datos que desaparecen más rápido (memoria RAM, conexiones de red activas) antes de pasar a los datos persistentes (discos duros, bitácoras archivadas).
 - Alineación Legal:** Los procedimientos deben cumplir con las leyes locales y los requisitos de los tribunales de justicia del país para que la evidencia sea admisible en caso de una demanda legal o penal contra el atacante o un empleado deshonesto.



Cláusula 5: Controles organizacionales

Control 5.28 Recopilación de evidencia

- Otra Información

Estándar Internacional de Referencia: Para la informática forense las directrices sugieren apoyarse de manera complementaria en la **norma ISO/IEC 27037**, la cual dicta las directrices específicas para el tratamiento de evidencia digital, también el **RFC 3227** Escrito por el Network Working Group de la IETF, funciona como una guía de mejores prácticas de alto nivel. Es considerado un estándar "de facto" pero no es una norma certificable

💡 **Prepara un "Kit de Primeros Auxilios Forenses" (Forensic Readiness):** TI debe contar con: herramientas de software libre o comerciales listas para usar (como FTK Imager o herramientas de volcado de RAM) instaladas en un dispositivo USB dedicado y protegido contra escritura. Si un servidor crítico es comprometido, el equipo técnico podrá extraer la evidencia de inmediato sin alterar el sistema operativo.

💡 **Documenta cada paso con capturas y firmas:** El registro de cadena de custodia debe incluir: la fecha exacta, la hora, el nombre del ingeniero, el número de serie del equipo afectado, el cálculo de hash del archivo copiado y las firmas de entrega y recepción. Si el auditor o un abogado notan un vacío de tiempo no justificado en el formato, toda la investigación perderá validez.

💡 **Capacita al personal en "No tocar":** El error más común de los administradores es: reiniciar un servidor comprometido para "ver si se arregla". Al hacer esto, borra de inmediato la memoria RAM, donde se almacenan las llaves de cifrado del ransomware o las conexiones activas del hacker. Entrena a tu equipo de soporte bajo una premisa simple, si sospechan de un ataque sofisticado, aíslan el equipo de la red pero déjenlo encendido para la llegada del analista forense.

💡 **Lo que el auditor te va a pedir en la práctica:** El auditor de la ISO 27001 querrá revisar: el formato oficial de cadena de custodia que tienes diseñado en tu sistema documental. Te preguntará: "Si descubren que un empleado filtró información confidencial y deciden rescindir su contrato, ¿cómo demuestran técnicamente que la evidencia que usaron para despedirlo no fue manipulada por el equipo de TI?". Mostrar tu procedimiento de copias forenses hashes y el formato de custodia firmado cerrará el control con éxito.



Cláusula 5: Controles organizacionales

Control 5.29 Seguridad de la información durante la interrupción

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

- **El Control:** La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante una interrupción.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar que, cuando ocurra una crisis, fallo de servicio, desastre natural o caída de sistemas, los controles de seguridad no se relajen de forma imprudente en el intento desesperado por restaurar las operaciones del negocio. Los puntos clave resumidos son:
 - Planificación de la Seguridad en Contingencias:** Identificar de antemano qué controles de seguridad deben mantenerse operativos de forma innegociable durante situaciones de emergencia o modos de operación degradados.
 - Preservación de la Confidencialidad e Integridad:** Evitar que los procedimientos manuales o de recuperación temporal expongan datos sensibles o permitan accesos no autorizados sin controles de autenticación.
 - Procesos de Autorización Excepcional:** Establecer protocolos claros para otorgar accesos de emergencia temporales sin romper la trazabilidad ni el registro de auditoría.
 - Capacitación y Pruebas Periódicas:** Entrenar al personal operativo en los procedimientos de seguridad en contingencia y validar los planes mediante ejercicios de simulación y simulacros de crisis.
 - Evaluación de Cambios en los Riesgos:** La dirección debe considerar que operar bajo un esquema de contingencia introduce nuevas amenazas (como accesos remotos inusuales o uso de equipos personales), las cuales deben ser analizadas y mitigadas de antemano.



Cláusula 5: Controles organizacionales

Control 5.29 Seguridad de la información durante la interrupción

- Otra Información

Relación con otros Estándares: Para una implementación robusta las directrices sugieren alinear este control con la norma **ISO 22301** (Sistemas de Gestión de Continuidad del Negocio), o bien la **ISO 27031** asegurando que la seguridad de la información sea un componente nativo de la resiliencia organizacional.

💡 **Define controles mínimos no negociables en tu BCP:** Documenta explícitamente en los planes de continuidad qué controles (como MFA, cifrado de bases de datos y registro de eventos) no pueden apagarse bajo ninguna circunstancia durante una caída.

💡 **Establece un procedimiento formal de 'Break-Glass':** Diseña cuentas de emergencia de contingencia con contraseñas resguardadas en bóveda digital y rotación automática, garantizando que su activación genere alertas inmediatas y auditoría completa.

💡 **Audita los procedimientos manuales de contingencia:** Si un proceso digital crítico pasa a ejecutarse en papel o planillas de cálculo locales durante una interrupción, implementa resguardo físico bajo llave y destrucción segura posterior.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el Plan de Continuidad del Negocio (BCP) y los Procedimientos de Seguridad de la Información en Situaciones de Emergencia. Para validar el control, revisará que los planes contemplen la protección de datos durante contingencias y no solo el restablecimiento de la disponibilidad; asimismo, solicitará los informes y bitácoras de los últimos simulacros de crisis o incidentes reales para constatar que los controles de acceso, el registro de eventos y los mecanismos de autorización se mantuvieron vigentes durante la interrupción y el retorno a la normalidad.



Cláusula 5: Controles organizacionales

Control 5.30 Preparación de las TIC para la continuidad del negocio

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

- **Control:** La organización debe planificar, implementar, mantener y probar la preparación de las TIC para la continuidad del negocio en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
- **Resumen de las Directrices de Implementación:** Este control exige pasar de las políticas de papel a la arquitectura técnica real, asegurando que la tecnología responda a las necesidades de disponibilidad determinadas por el Análisis de Impacto al Negocio (BIA):
 - Determinación de Métricas RTO y RPO:**
 - RTO (Recovery Time Objective):** El tiempo máximo tolerable que un sistema puede estar caído antes de causar un daño inaceptable.
 - RPO (Recovery Point Objective):** La cantidad máxima de datos que la empresa se puede permitir perder (medido en tiempo de transacciones/respaldos).
 - Arquitectura de Alta Disponibilidad:** Se deben diseñar e implementar: redundancias en los componentes críticos de TI, tales como fuentes de poder dobles, múltiples proveedores de internet, clústeres de servidores y almacenamiento en espejo (mirroring).
 - Planes de Continuidad de TIC (DRP):** Se deben documentar los pasos técnicos específicos para restaurar la infraestructura tecnológica, los sistemas operativos, las bases de datos y los enlaces de telecomunicaciones.
 - Programa de Pruebas Periódicas:** La infraestructura de respaldo debe probarse formalmente a intervalos planificados para validar que los tiempos de recuperación reales coinciden con las métricas teóricas aprobadas por la dirección.



Cláusula 5: Controles organizacionales

Control 5.30 Preparación de las TIC para la continuidad del negocio

- Otra Información

Relación con otros Estándares: Para una implementación robusta las directrices sugieren alinear este control con la norma **ISO 22301** (Sistemas de Gestión de Continuidad del Negocio), o bien la **ISO 27031** asegurando que la seguridad de la información sea un componente nativo de la resiliencia organizacional.

💡 **Calcula y formaliza RTO y RPO con los dueños del proceso:** No asumas parámetros técnicos en TI por cuenta propia; valida con la dirección financiera y de operaciones cuánto tiempo de inactividad (RTO) y cuántas horas/minutos de pérdida de transacciones (RPO) puede tolerar la empresa antes de sufrir pérdidas irreversibles.

💡 **Automatiza los ejercicios de conmutación por error (Failover):** Diseña pruebas periódicas donde fuerces la caída de un servidor primario o nodo de base de datos para verificar que el tráfico se desvíe automáticamente al sitio secundario sin intervención manual propensa a errores.

💡 **Documenta procedimientos de recuperación con dependencias jerárquicas:** Un DRP falla si los ingenieros intentan encender las aplicaciones antes que los controladores de dominio (DNS/Active Directory) o las bases de datos; grafica claramente el orden estricto de arranque de los servicios en el manual de crisis.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el Plan de Recuperación ante Desastres de TI (DRP), el Análisis de Impacto en el Negocio (BIA) donde se definan formalmente los RTO y RPO por activo, y el cronograma anual de pruebas de continuidad. Para evaluar la efectividad real, pedirá las evidencias y reportes técnicos del último simulacro de recuperación o ejercicio de conmutación (failover report); el auditor verificará si los tiempos cronometrados de restablecimiento y la integridad de los datos recuperados se mantuvieron estrictamente dentro de los umbrales de RTO y RPO aprobados por la dirección.



Cláusula 5: Controles organizacionales

Control 5.31 Requisitos legales, estatutarios, regulatorios y contractuales

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

- **Control:** La organización debe identificar explícitamente y mantener actualizados todos los requisitos legales, estatutarios, regulatorios y contractuales pertinentes a la seguridad de la información, así como el enfoque de la organización para cumplir con estos requisitos.
- **Resumen de las Directrices de Implementación:** Este control exige que la seguridad de la información no opere en el vacío, sino totalmente alineada con el entorno legal donde tiene presencia el negocio:
 - Matriz de Cumplimiento:** La organización debe desarrollar un inventario documentado que liste todas las leyes nacionales e internacionales, regulaciones de su sector industrial y contratos con clientes que incluyan obligaciones de ciberseguridad.
 - Actualización Continua:** Los procesos internos deben garantizar el monitoreo periódico de los cambios legislativos para adaptar las políticas del Sistema de Gestión de la Seguridad de la Información (SGSI) antes de que las nuevas leyes entren en vigor.
 - Propiedad Intelectual:** Se deben implementar controles específicos para proteger los derechos de autor, patentes, marcas comerciales y el uso de licencias de software legítimas, prohibiendo estrictamente el material pirateado.
 - Protección de Registros Organizacionales:** Los datos esenciales deben resguardarse contra pérdida, destrucción y falsificación, cumpliendo con los tiempos de retención mínimos exigidos por las leyes fiscales, comerciales o laborales aplicables.



Cláusula 5: Controles organizacionales

Control 5.31 Requisitos legales, estatutarios, regulatorios y contractuales

- Otra Información

Privacidad de Datos Personales: Este control se conecta directamente con leyes internacionales de privacidad de datos (como el RGPD europeo, legislaciones locales de protección de datos o normativas financieras), exigiendo responsabilidades penales y administrativas muy estrictas a los directivos si ocurre una brecha.

💡 **Diseña una Matriz de Cumplimiento Regulatorio viva:** El error organizativo más común es dejar la identificación de las leyes en un párrafo de texto plano dentro de una política que nadie lee. Crea una tabla formal administrada en conjunto por el área legal y el equipo de seguridad que desglose: 1) Nombre de la ley/regulación, 2) Artículo o cláusula específica de seguridad, 3) Control técnico o administrativo con el que tu empresa lo cumple, y 4) Fecha de la última revisión.

💡 **Audita el uso de software sin licencia:** La gestión de activos debe incluir herramientas automatizadas que escaneen los equipos de la organización en busca de programas no autorizados o crackeados.

💡 **Configura políticas de retención y borrado automático:** Los sistemas de almacenamiento deben programarse para cumplir estrictamente con los plazos legales de retención de documentos. Por ejemplo, si las leyes fiscales exigen conservar los archivos contables por 5 años, configura tu repositorio para congelar esos datos durante ese periodo y destruirlos de manera segura automáticamente al cumplirse el plazo, minimizando la superficie de riesgo en caso de una filtración de datos.

💡 **Lo que el auditor te va a pedir en la práctica:** El auditor de la ISO 27001 solicitará tu matriz de requisitos legales aplicables al alcance del SGSI. Te pedirá una prueba de campo "Ustedes manejan datos personales de clientes en su plataforma; muéstrenme bajo qué ley local o internacional se fundamenta su aviso de privacidad y cómo aseguran técnicamente que el usuario pueda ejercer su derecho a eliminar sus datos del sistema". Si le muestras el inventario legal actualizado y el flujo técnico que respalda el cumplimiento de esa normativa, el control estará plenamente aprobado.



Cláusula 5: Controles organizacionales

Control 5.32 Derechos de propiedad intelectual

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

- **Control:** La organización debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
- **Resumen de las Directrices de Implementación:** Este control exige la protección de los activos intelectuales de la empresa y el respeto a las licencias de propiedad ajena:
 - Política de propiedad intelectual:** reglas institucionales para el uso correcto de software, libros, música y patentes dentro de la empresa.
 - Inventario de licencias:** registro técnico que demuestra la legalidad de todo el software comercial instalado en los equipos de la organización.
 - Protección del código fuente:** controles de acceso y cifrado para resguardar las aplicaciones creadas por la empresa frente a plagios o robos.
 - Cláusulas laborales:** acuerdos firmados con empleados y contratistas que establecen que todo desarrollo creado durante su jornada laboral pertenece a la empresa.
 - Límites de copia:** prohibición explícita de duplicar material protegido por derechos de autor sin la autorización del creador.



Cláusula 5: Controles organizacionales

Control 5.32 Derechos de propiedad intelectual

- Otra Información

Riesgo por infracción: advertencia sobre las consecuencias legales, penales y de reputación que sufre una organización si utiliza herramientas pirateadas o distribuye contenido sin derechos de autor.

💡 **Implementa un sistema SAM (Software Asset Management):** herramientas de software automatizadas que escanean de forma continua las computadoras de la red corporativa para detectar y bloquear programas no autorizados, piratas o que carezcan de una licencia comercial vigente.

💡 **Establece la firma obligatoria de NDAs y convenios de propiedad:** documentos legales integrados al contrato de trabajo de todos los ingenieros y desarrolladores para blindar la autoría de los sistemas que construyan para el negocio.

💡 **Configura repositorios centralizados de código:** plataformas técnicas con permisos de lectura restringidos que impiden la descarga masiva de código fuente por parte de usuarios externos.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Propiedad Intelectual y Gestión de Licencias de Software, así como el inventario actualizado de activos de software vs. facturas de compra. Durante la auditoría, seleccionará una muestra de servidores y computadoras de usuarios para auditar el software instalado; comprobará que no exista software pirata, revisará los contratos de desarrolladores para validar las cláusulas de cesión de propiedad intelectual y pedirá evidencias de las revisiones periódicas de cumplimiento de licenciamiento comercial y de código abierto.



Cláusula 5: Controles organizacionales

Control 5.33 Protección de registros

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

- **Control:** La organización debe proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y comerciales.
- **Resumen de las Directrices de Implementación:** Este control exige una gestión estructurada de los registros del negocio (facturas, contratos, auditorías, bitácoras de sistemas):
 - Política de retención:** calendario documentado que establece el tiempo mínimo y máximo de conservación para cada tipo de registro.
 - Clasificación de registros:** categorización de la información según su valor legal, fiscal, operativo o histórico.
 - Control de integridad:** mecanismos criptográficos o físicos que impiden la alteración o falsificación de los documentos guardados.
 - Destrucción segura:** procedimientos técnicos para eliminar de forma definitiva los registros una vez cumplido su tiempo de vida legal.
 - Pruebas de legibilidad:** revisiones periódicas para comprobar que los archivos antiguos almacenados en medios digitales sigan siendo accesibles con la tecnología actual.



Cláusula 5: Controles organizacionales

Control 5.33 Protección de registros

- Otra Información

Formatos físicos y digitales: aclaración normativa que extiende la obligatoriedad de la protección tanto a los archivos guardados en bases de datos y nubes como a los documentos en papel archivados en bodegas físicas.

💡 **Implementa políticas de inmutabilidad (WORM):** configuración de almacenamiento tecnológico (Write Once, Read Many) aplicada a los repositorios de bitácoras y registros críticos que impide que cualquier usuario, incluso un administrador del sistema, pueda borrar o modificar los archivos guardados.

💡 **Establece un inventario automatizado de retención:** bases de datos parametrizadas con alertas de calendario que notifican al oficial de cumplimiento el momento exacto en que un bloque de documentos fiscales o laborales ha cumplido su plazo legal y puede proceder a su trituración o borrado seguro.

💡 **Lo que el auditor te va a pedir en la práctica:** evidencia de cumplimiento de los plazos de conservación. El auditor te solicitará tu política de retención de registros, elegirá una categoría (como los registros de nómina o contratos de proveedores de hace tres años) y te dirá: "Muéstreme dónde están almacenados estos registros específicos, quién tiene permisos para verlos y cómo garantizan que no hayan sido alterados desde su creación". Mostrar las bitácoras de acceso al repositorio y las firmas hash de los archivos validará el control.



Cláusula 5: Controles organizacionales

Control 5.34 Privacidad y protección de información de identificación personal (PII)

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

- **Control:** La organización debe identificar e implementar los requisitos para la privacidad y la protección de la información de identificación personal (PII) de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
- **Resumen de las Directrices de Implementación:** Este control exige un marco de gobernanza específico para salvaguardar los datos de personas físicas garantizando su privacidad:
 - Política de privacidad:** documento institucional que dicta las reglas de recolección, uso, almacenamiento y destrucción de datos personales.
 - Roles de privacidad:** designación formal de figuras responsables como el Oficial de Protección de Datos (DPO).
 - Derechos de los titulares:** mecanismos técnicos para que los usuarios puedan ejercer su derecho a acceder, rectificar, cancelar u oponerse al uso de sus datos.
 - Evaluación de Impacto (PIA):** análisis previo de los riesgos de privacidad antes de implementar nuevos sistemas que procesen datos personales masivos.
- **Consentimiento explícito:** procesos para obtener la autorización informada y demostrable del usuario antes de capturar sus datos.



Cláusula 5: Controles organizacionales

Control 5.34 Privacidad y protección de información de identificación personal (PII)

- Otra Información

Estándar de Extensión: referencia técnica que recomienda adoptar la norma ISO/IEC 27701 (Sistema de Gestión de Información de Privacidad - PIMS) si la organización procesa volúmenes críticos de PII de forma nativa.

💡 **Implementa la Privacidad desde el Diseño:** configuración técnica que garantiza que cualquier software nuevo recolecta únicamente los datos personales mínimos necesarios para operar, bloqueando campos excesivos por defecto.

💡 **Cifra la PII en tránsito y reposo:** uso obligatorio de algoritmos avanzados (como AES-256) en las bases de datos y protocolos seguros (como HTTPS) en formularios web para volver ilegible la información ante filtraciones.

💡 **Automatiza el borrado por inactividad:** herramientas de software programadas para anonimizar o destruir registros de clientes que han estado inactivos durante el tiempo límite establecido por la ley.

💡 **Lo que el auditor te va a pedir en la práctica:** evidencia del flujo de un dato personal dentro de tu organización. El auditor elegirá el registro de un cliente al azar y te preguntará: "¿Dónde está el consentimiento explícito que firmó este usuario y cómo demuestran que pueden borrarlo por completo del sistema si él lo solicita?". Mostrar el mapa de datos y el flujo de atención a solicitudes de privacidad validará el control.



Cláusula 5: Controles organizacionales

Control 5.35 Revisión independiente de la seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Cor- correctivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Information_secu- rity_assurance	# Gobernanza_y_ Ecosistema

- **Control:** La organización debe revisar el enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos de seguridad de la información) de forma independiente a intervalos planificados o cuando ocurran cambios significativos.
- **Resumen de las Directrices de Implementación:** Este control exige auditorías y evaluaciones ciegas para asegurar que la seguridad de la empresa no se base en la autoevaluación de quienes diseñaron los controles:
 - Intervalos planificados:** calendario obligatorio que define la ejecución de revisiones exhaustivas al por ejemplo una vez al año.
 - Independencia del revisor:** selección de auditores internos que no gestionen los controles evaluados, o la contratación de firmas de consultoría externas.
 - Eventos desencadenantes:** obligación de iniciar una revisión inmediata tras cambios mayores en la infraestructura, incidentes de seguridad graves o nuevas regulaciones legales.
 - Informes a la alta dirección:** presentación formal de los hallazgos, vulnerabilidades descubiertas y desviaciones normativas ante el comité directivo.
 - Seguimiento de acciones:** registro auditable de los planes de remediación diseñados para corregir las fallas detectadas por el revisor independiente.



Cláusula 5: Controles organizacionales

Control 5.35 Revisión independiente de la seguridad de la información

- Otra Información

Diferencia con la revisión por la dirección: aclaración técnica que distingue este control (enfocado en la verificación técnica y operativa objetiva) del proceso de revisión directiva ejecutado por los líderes del negocio.

💡 **Garantiza la imparcialidad cruzando auditores:** enfoque organizativo aplicable si no cuentas con presupuesto para contratar auditores externos, el cual consiste en capacitar como auditores internos al personal de un área (como Calidad o Finanzas) para que evalúen a TI y Seguridad, asegurando que nadie audite su propio trabajo.

💡 **Lo que el auditor te va a pedir en la práctica:** evidencia de la ejecución de la última revisión independiente realizada y te dirá: "Muéstreme evidencia que ejecutó esta revisión para validar su independencia, y la evidencia de cómo solucionaron las observaciones críticas detectadas en el reporte". Mostrar el plan de revisión firmado y los tickets cerrados de remediación validará el control.



Cláusula 5: Controles organizacionales

Control 5.36 Cumplimiento de políticas y normas de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Capacidad operativa dades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Legal_and_compliance # Information_security_assurance	# Gobernanza_y_Ecosistema

- **Control:** La organización debe revisar periódicamente el cumplimiento de las políticas, directrices y normas de seguridad de la información pertinentes de la organización.
- **Resumen de las Directrices de Implementación:** Este control exige revisiones técnicas regulares para confirmar que las configuraciones reales de los servidores, redes y aplicaciones no se hayan desviado de lo estipulado en las políticas internas:
 - Revisiones técnicas automatizadas:** uso de herramientas de escaneo para validar las configuraciones de los sistemas frente a líneas base de seguridad.
 - Supervisión de los administradores:** obligación de los gerentes de TI de verificar que su propio personal operativo aplique los parches y reglas de seguridad correspondientes.
 - Manejo de desviaciones:** procesos formales para registrar, justificar y autorizar excepciones temporales si un sistema no puede cumplir con una norma técnica por restricciones operativas.
 - Acciones correctivas inmediatas:** aplicación de remediaciones técnicas si se detecta un servidor desactualizado, un puerto abierto no autorizado o un usuario con privilegios excesivos.



Cláusula 5: Controles organizacionales

Control 5.36 Cumplimiento de políticas y normas de seguridad de la información

- Otra Información

Diferencia con la auditoría independiente: aclaración normativa que distingue este control (una verificación técnica y operativa rutinaria hecha por el propio equipo de TI/Seguridad) del Control 5.35 (una evaluación imparcial hecha por ojos externos).

💡 **Utiliza herramientas de cumplimiento de configuración (Configuration Compliance):** plataformas de software programadas para analizar de forma automática los servidores de la empresa y lanzar alertas inmediatas si un ingeniero cambia una regla del firewall o desactiva un cifrado obligatorio, violando la política interna.

💡 **Establece plantillas de endurecimiento técnicas (Hardening Standards):** guías de configuración específicas para cada tecnología (como Linux, Windows Server, AWS) que los administradores de sistemas deben aplicar de forma obligatoria antes de liberar cualquier equipo al entorno de producción.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el procedimiento o calendario formal de revisiones de cumplimiento de políticas internas. Para validar su aplicación práctica, pedirá las evidencias de las últimas revisiones ejecutadas (reportes de configuración técnica, listas de verificación operativas firmadas y minutas de seguimiento); comprobará que existan métricas de adhesión a las políticas y revisará el registro de no conformidades o desviaciones detectadas para constatar que se implementaron planes de acción correctiva eficaces.



Cláusula 5: Controles organizacionales

Control 5.37 Procedimientos operativos documentados

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Recuperar	# Gestión de activos # Seguridad física # sistema_y_red-trabajo_seguridad #Aplicación_seguridad # configuración_segura #Identidad_y_acceso_administración # Threat_and_vulnerability_management # Continuidad # Information_security_event_management	# Gobernanza_y_Ecosistema # Protección # Defensa

- **Control:** Los procedimientos operativos para las actividades de procesamiento de información deben documentarse y ponerse a disposición de todas las personas que los necesiten.
- **Resumen de las Directrices de Implementación:** Este control exige que la operación diaria de la tecnología no dependa de la memoria o el humor de los ingenieros, sino de manuales e instrucciones claras que garanticen la ejecución segura y repetible de las tareas:



Cláusula 5: Controles organizacionales

Control 5.37 Procedimientos operativos documentados

- Contenido de los procedimientos:** manuales que detallan actividades críticas como el encendido y apagado de sistemas, el procesamiento de datos, el mantenimiento de equipos y la gestión de fallas.
- Instrucciones de respaldo:** guías paso a paso para la ejecución, verificación y almacenamiento seguro de las copias de seguridad de la empresa.
- Programación de tareas:** calendarios y especificaciones técnicas para la ejecución de trabajos por lotes (batch processing) y la administración de dependencias del sistema.
- Gestión de excepciones:** instrucciones claras sobre qué debe hacer el operador si una tarea automatizada falla o arroja un error inusual.
- Control de acceso a manuales:** disponibilidad de las guías únicamente para el personal autorizado que opera directamente las plataformas, evitando la exposición innecesaria de la arquitectura interna.

- **Otra Información**

Sistemas heredados y automatización: aclaración normativa que impulsa a las organizaciones a automatizar la mayor cantidad de procedimientos operativos posibles mediante scripts o herramientas de orquestación, reduciendo el error humano y la necesidad de documentación manual interactiva.



Cláusula 5: Controles organizacionales

Control 5.37 Procedimientos operativos documentados

💡 **Crea una biblioteca centralizada de Runbooks:** uso de plataformas wiki corporativas protegidas (como Confluence o repositorios Git internos) donde los ingenieros puedan consultar y actualizar las guías operativas de forma rápida, eliminando los archivos PDF locales o desactualizados en las computadoras personales.

💡 **Escribe los manuales pensando en el peor escenario:** redacción técnica estructurada bajo la premisa de que el ingeniero experto no estará disponible durante una falla. Los procedimientos deben incluir capturas de pantalla, comandos exactos y árboles de decisión sencillos para que un técnico de nivel básico pueda ejecutar la tarea de forma segura a mitad de la noche.

💡 **Implementa control de versiones estricto en los scripts:** políticas de gobernanza para cualquier archivo de automatización o código de infraestructura (Infrastructure as Code) que exigen que cada cambio operativo sea revisado por un segundo ingeniero antes de ser aplicado en el entorno de producción.

💡 **Lo que el auditor te va a pedir en la práctica:** evidencia de que la operación sigue un estándar documentado. El auditor seleccionará un proceso crítico del alcance (como la creación de un nuevo usuario en la base de datos o el mantenimiento mensual del servidor de correo) y te dirá: "Muéstreme el manual operativo escrito para esta tarea y el registro o ticket que demuestre que el técnico ejecutó los pasos exactamente como dicta su procedimiento". Mostrar la coincidencia exacta entre el manual y la bitácora de ejecución aprobará el control.



Cláusula 6: Controles de personas

Control 6.1 Screening

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

- **Control:** Las verificaciones de antecedentes de todos los candidatos a empleados, contratistas y usuarios de terceras partes deben realizarse antes de incorporarse a la organización y de forma continua, de manera proporcional a los requisitos del negocio, la clasificación de la información a la que se accederá y los riesgos percibidos
- **Resumen de las Directrices de Implementación:** Este control busca asegurar que las personas que ingresan a la organización (o que cambian de rol dentro de ella) sean idóneas y confiables. Las directrices clave para su implementación son:
 - Definición de Niveles de Riesgo:** El proceso de tamizado no debe ser igual para todos. Se debe estructurar según la criticidad del puesto y el nivel de acceso a la información confidencial.
 - Elementos del Tamizado Inicial Antes de la contratación o asignación, se deben verificar de forma estándar:**
 - Identidad de la persona (documentos oficiales, pasaporte, etc.).
 - Referencias académicas y profesionales (títulos, cartas de recomendación).
 - Historial laboral declarado.



Cláusula 6: Controles de personas

Control 6.1 Screening

-Verificaciones Avanzadas: Para roles de alta responsabilidad, acceso a datos sensibles o privilegios de administrador, se puede incluir (siempre bajo el marco legal local):

- Verificaciones de antecedentes penales o judiciales.

- Comprobaciones de historial crediticio o financiero (si aplica a funciones financieras).

-Evaluación Continua (On-going screening): El tamizado no es un evento único. Se debe repetir periódicamente o cuando ocurran eventos significativos (ej. un ascenso, cambio de responsabilidades, o sospecha de incidentes).

-Contratistas y Terceras Partes: Los acuerdos con proveedores deben exigir por contrato que estos realicen un tamizado equivalente a su personal antes de que tengan acceso a los activos de la organización.

- **Otra Información**

Cumplimiento Legal y Privacidad: Las prácticas de tamizado deben respetar rigurosamente la legislación local, las leyes de protección de datos personales y los derechos humanos. No se pueden solicitar datos biométricos, médicos o de antecedentes sin el consentimiento explícito y la justificación legal adecuada.

Documentación del Proceso: La organización debe documentar los criterios de idoneidad, quién realiza las verificaciones y dónde se almacenan de forma segura los resultados (normalmente en el área de Capital Humano).



Cláusula 6: Controles de personas

Control 6.1 Screening

💡 **Hazlo a la medida:** Automatiza un sistema de clasificación de puestos junto a Recursos Humanos. Un desarrollador con acceso a las bases de datos de producción necesita un tamizado mucho más riguroso que un rol operativo sin acceso a datos críticos.

💡 **Cuidado con el limbo legal:** Asegúrate de que el candidato firme un consentimiento explícito de verificación de antecedentes antes de mover un solo dedo. En muchas legislaciones, investigar la vida privada, financiera o judicial de alguien sin su autorización por escrito puede acarrear multas severas de protección de datos que costarían más que el riesgo que intentas prevenir.

💡 **El tamizado continuo es el verdadero reto:** El error más común es revisar al empleado cuando entra y olvidarse de él por diez años. Implementa "disparadores" automatizados; por ejemplo, si un empleado es promovido a un puesto clave o si sufre un cambio drástico en sus privilegios de acceso al sistema, el sistema de RR.HH.

💡 **Blinda la cadena de suministro con contratos claros:** Cuando utilices outsourcing o consultores externos, traslada la responsabilidad legal. Exige en las cláusulas del contrato (SLA) que la empresa proveedora demuestre que realiza el tamizado a su personal bajo los mismos estándares que tú, y resérvate el derecho de auditar esas evidencias cuando lo consideres necesario.

💡 **El enfoque del auditor (Lo que te van a revisar):** El auditor validará este control mediante un muestreo cruzado de empleados, contratistas y personal promovido, donde exigirá ver la matriz de criticidad de puestos para confirmar que el nivel de investigación es proporcional al riesgo de cada rol. Revisará minuciosamente que las fechas de los reportes de antecedentes (identidad, referencias y judiciales) sean anteriores a la fecha de contratación o de asignación de accesos al sistema, buscando cualquier brecha temporal que haya expuesto la información. Asimismo, te pedirá los consentimientos firmados por escrito de los candidatos para asegurar la legalidad del proceso, y pondrá especial lupa en los contratos y acuerdos de nivel de servicio (SLA) con proveedores y terceras partes, exigiendo evidencias documentales de que ellos también tamizan a su personal antes de permitirles interactuar con tus activos de información.



Cláusula 6: Controles de personas

Control 6.2 Términos y condiciones del empleo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

- **Control:** Los acuerdos contractuales con el personal deben establecer sus responsabilidades y las de la organización en relación con la seguridad de la información.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en que las obligaciones de seguridad deben ser legalmente vinculantes desde el inicio de la relación laboral. Los puntos clave resumidos son:
 - Compromiso Contractual:** Las responsabilidades de seguridad de la información deben quedar plasmadas explícitamente en el contrato de trabajo, en los términos de condiciones o en un acuerdo de confidencialidad (NDA) anexo, el cual debe ser firmado por el colaborador antes de acceder a los activos.
 - Claridad en las Obligaciones:** El contrato o anexo debe especificar el deber del empleado de salvaguardar la información confidencial, clasificar los datos de manera adecuada, seguir las políticas de uso aceptable de activos y notificar de inmediato cualquier incidente o debilidad de seguridad observada.
 - Permanencia en el Tiempo:** Se debe estipular explícitamente que la responsabilidad de confidencialidad y protección de ciertos datos clave de la organización continúa vigente durante un período definido de tiempo después de que la relación laboral o contractual haya finalizado.
 - Consecuencias del Incumplimiento:** El acuerdo debe definir claramente las acciones disciplinarias o legales aplicables en caso de que el colaborador ignore o viole de forma deliberada las políticas de seguridad de la información establecidas por la empresa.



Cláusula 6: Controles de personas

Control 6.2 Términos y condiciones del empleo

- **Otra Información:** La norma recuerda que las organizaciones pueden requerir que los empleados firmen declaraciones de confidencialidad o actualizaciones de sus acuerdos contractuales de forma periódica. Esto es especialmente relevante cuando ocurren cambios significativos en las funciones del puesto, nuevas regulaciones legales o reestructuraciones tecnológicas importantes dentro del negocio.

💡 **Integra la seguridad en el onboarding legal:** No permitas que el área legal utilice contratos genéricos que omitan el entorno digital actual. Trabaja en equipo para que todo nuevo contrato contenga cláusulas robustas sobre el uso correcto de credenciales, propiedad intelectual del código o datos generados, y la prohibición estricta de extraer información a cuentas personales.

💡 **El NDA no es solo para el ingreso:** Asegúrate de que los Acuerdos de Confidencialidad (NDAs) tengan validez jurídica posterior al empleo (post-employment). Es vital que el colaborador firme y entienda que los secretos comerciales, bases de datos de clientes o estrategias de TI que conoció durante su estancia no pueden ser divulgados ni utilizados en su próximo empleo.

💡 **Haz las políticas accesibles y referenciadas:** En lugar de saturar el contrato de trabajo con 50 páginas de reglas técnicas, incluye una cláusula donde el empleado declare conocer, entender y comprometerse a cumplir la "Política General de Seguridad de la Información" de la empresa, ligando legalmente el contrato laboral con tus políticas vivas de TI.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor le solicitará a RH una muestra de contratos laborales vigentes y convenios de confidencialidad firmados tanto por personal interno como por contratistas externos para comprobar la existencia de las cláusulas de seguridad y secreto profesional. Revisará que las fechas de firma de dichos documentos sean anteriores al primer día de trabajo o a la fecha de creación de los accesos lógicos del usuario, y verificará que el reglamento interior de trabajo (o el código de conducta) se encuentre formalmente vinculado al contrato legal, garantizando así que la organización cuenta con el sustento jurídico para aplicar medidas disciplinarias en caso de un incidente de seguridad provocado por negligencia del personal.



Cláusula 6: Controles de personas

Control 6.3 Concientización, educación y capacitación en seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

- **El Control:** El personal de la organización y las partes interesadas pertinentes deben recibir concientización, educación y capacitación adecuadas en seguridad de la información, así como actualizaciones periódicas de las políticas de seguridad de la información de la organización, políticas específicas y procedimientos, según sea relevante para su función laboral.
- **Resumen de las Directrices de Implementation:** El error humano es uno de los vectores de ataque más comunes, por lo que se debe estructurar un programa continuo y dinámico que transforme la cultura de seguridad. Los puntos clave resumidos son:
 - Programa de Concientización Basado en Roles:** La capacitación no debe ser genérica. Se deben diseñar perfiles de entrenamiento según la función; por ejemplo, los desarrolladores necesitan capacitación en desarrollo seguro, mientras que los ejecutivos requieren enfoque en fraudes de alta dirección (CEO Fraud).
 - Frecuencia y Actualización:** No es una actividad de una sola vez al año. El programa debe ser continuo y actualizarse cuando ocurran cambios en las políticas, se detecten nuevas amenazas en el mercado o se implementen nuevas tecnologías en la empresa.
 - Inducción Inmediata (Onboarding):** Todo nuevo colaborador debe recibir una concientización sobre las reglas básicas de seguridad al asumir sus funciones.
 - Evaluación de la Efectividad:** La organización debe medir si la capacitación está funcionando. Esto se logra mediante exámenes de conocimiento, métricas de asistencia o, de manera más práctica, a través de simulacros periódicos de ataques controlados (como campañas de phishing simuladas).



Cláusula 6: Controles de personas

Control 6.3 Concientización, educación y capacitación en seguridad de la información

- **Otra Información:** La norma señala que un buen programa de concientización debe utilizar múltiples canales de comunicación (boletines, videos cortos, talleres interactivos) para mantener el interés del personal. Además, resalta la importancia de extender estas actividades a terceros o contratistas externos que tengan acceso a los sistemas internos de la organización, adaptando el contenido a su nivel de interacción.

💡 **Apuesta por el microaprendizaje y la gamificación:** Olvídate de los aburridos cursos de tres horas que los empleados reproducen en segundo plano sin prestar atención. Implementa cápsulas de video de 5 minutos, infografías dinámicas y cuestionarios con recompensas (gamificación) que mantengan al personal enganchado y refuercen la cultura de ciberseguridad mes con mes.

💡 **Los simulacros de phishing son tu mejor termómetro:** No midas el éxito de tu programa solo con una lista de asistencia. Diseña campañas internas de phishing ético; si el porcentaje de clics en enlaces sospechosos disminuye con el tiempo, sabrás con datos reales que tu estrategia de concientización está funcionando y dónde necesitas reforzar.

💡 **Involucra a los líderes como ejemplo:** La seguridad de la información se adopta de arriba hacia abajo. Asegúrate de que los directores y gerentes de área sean los primeros en completar los entrenamientos y promover las buenas prácticas; cuando el equipo ve que sus líderes se toman en serio la protección de datos, la cultura organizacional cambia por completo.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor te solicitará el programa anual de concientización en seguridad de la información y buscará evidencia de su ejecución, tales como listas de asistencia, calificaciones de exámenes o constancias de los cursos tomados por el personal seleccionado en su muestra. Asimismo, revisará los resultados de las métricas de efectividad (por ejemplo, los reportes de las campañas de phishing simuladas) para verificar que la organización toma acciones correctivas con aquellos usuarios que reprueban o caen constantemente en las trampas, demostrando así que el proceso de capacitación es un ciclo de mejora continua y no un simple requisito de papel.



Cláusula 6: Controles de personas

Control 6.4 Proceso disciplinario

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

- **El Control** :Se debe 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 seguridad de la información.
- **Resumen de las Directrices de Implementación:** La guía establece que las políticas de seguridad pierden efectividad si su incumplimiento no genera consecuencias. Por ello, se debe estructurar un mecanismo sancionatorio claro y justo. Los puntos clave resumidos son:
 - Formalización del Proceso:** La organización debe contar con un procedimiento oficial, documentado y legalmente respaldado que defina las etapas del proceso disciplinario ante una falta a las políticas de seguridad de la información.
 - Gradualidad y Proporcionalidad:** Las sanciones deben ser proporcionales a la gravedad de la infracción, la intencionalidad del colaborador, el impacto del daño causado y si se trata de una primera falta o de una reincidencia. La escala suele ir desde amonestaciones verbales o escritas, hasta la rescisión laboral o acciones legales.
 - Comunicación Transparente:** El proceso y las posibles consecuencias deben ser informados a todo el personal de manera clara y abierta (por ejemplo, a través del reglamento interior de trabajo) para que sirva como un mecanismo de disuasión eficaz.
 - Debido Proceso:** Se debe garantizar una investigación justa, objetiva e independiente antes de aplicar cualquier sanción, otorgando al colaborador el derecho a ser escuchado y a presentar sus argumentos o pruebas.



Cláusula 6: Controles de personas

Control 6.4 Proceso disciplinario

- **Otra Información:** La norma resalta que este proceso también debe considerar la desconexión inmediata o la revocación de accesos lógicos y físicos de forma preventiva mientras se realiza la investigación de un incidente grave. Además, se señala que el proceso disciplinario debe poder aplicarse de manera equivalente a contratistas y personal externo, comúnmente mediante cláusulas de penalización financiera o la terminación del contrato comercial con el proveedor.

💡 **Alineación total con la legislación laboral:** No diseñes sanciones de seguridad en una burbuja de TI. Trabaja de la mano con el departamento legal y de Recursos Humanos para asegurarte de que tu escala de sanciones esté perfectamente integrada en el Reglamento Interior de Trabajo depositado ante las autoridades laborales; de lo contrario, cualquier despido por violar la seguridad de la información podría ser catalogado como injustificado.

💡 **Distingue entre error humano y negligencia:** Tu proceso disciplinario debe ser justo. Si un empleado cae en un ataque de phishing de ingeniería social sumamente sofisticado, requiere capacitación y refuerzo, no un castigo; pero si un colaborador desactiva deliberadamente el antivirus o extrae información confidencial en una memoria USB sabiendo que está prohibido, la sanción debe ser contundente.

💡 **Utiliza el proceso como un elemento disuasorio:** El objetivo del control no es castigar a todos, sino prevenir incidentes. Publicar de manera interna las consecuencias generales o estadísticas de las malas prácticas ayuda a que toda la organización entienda que las políticas de seguridad se monitorean activamente y se toman en serio.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el Reglamento Interior de Trabajo, la política de sanciones o el procedimiento disciplinario formalizado para constatar que las violaciones a la seguridad de la información están explícitamente tipificadas. Posteriormente, pedirá evidencia de su comunicación al personal y, en caso de que hayan ocurrido incidentes de seguridad causados por el personal en el último año, revisará los expedientes de dichos casos para verificar que se siguió el debido proceso de investigación documentado, que se aplicaron las sanciones correspondientes según la gravedad de la falta.



Cláusula 6: Controles de personas

Control 6.5 Responsabilidades después de la terminación o cambio de empleo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad # Gestión de activos	# Gobernanza_y_ Ecosistema

- **El Control:** Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo deben definirse, comunicarse al personal y a otras partes interesadas pertinentes, y hacerse cumplir.
- **Resumen de las Directrices de Implementación:** La guía de implementación se centra en mitigar el riesgo de fuga de información o accesos no autorizados cuando un colaborador deja la empresa o cambia de área interna. Los puntos clave resumidos son:
 - Proceso de Salida Estructurado (Offboarding):** La organización debe contar con un procedimiento formal para la baja de empleados o contratistas. Este proceso debe asegurar la devolución inmediata de todos los activos físicos (computadoras, tokens, identificaciones) y la revocación de todos los accesos lógicos (correos, VPN, bases de datos).
 - Responsabilidades Post-Empleo:** Se debe recordar explícitamente al colaborador saliente que sus obligaciones de confidencialidad y secreto profesional se mantienen vigentes incluso después de que termine la relación laboral, por el tiempo estipulado en su contrato original o NDA.
 - Cambios de Rol Internos (Movilidad):** El control también aplica cuando un empleado cambia de puesto dentro de la misma empresa.
 - Notificación y Documentación:** Se debe asignar una figura responsable (usualmente una lista de verificación compartida entre TI y Recursos Humanos) que registre y documente formalmente el cierre de cada cuenta y la recepción conforme de los activos devueltos.



Cláusula 6: Controles de personas

Control 6.5 Responsabilidades después de la terminación o cambio de empleo

- **Otra Información:** La norma advierte que el incumplimiento de este control suele ser una de las principales causas de incidentes de seguridad (fuga de propiedad intelectual o sabotaje por parte de ex-empleados resentidos). También destaca la importancia de notificar a los clientes o proveedores externos clave cuando un punto de contacto principal de la organización ha sido dado de baja o cambiado de puesto, evitando así suplantaciones de identidad.

💡 **Automatiza la revocación con un Check-list digital:** No confíes la baja de accesos a la memoria del administrador de sistemas. Implementa un flujo automatizado o una lista de verificación digital (Check-list de Offboarding) vinculada entre Recursos Humanos y TI que garantice que, en el minuto exacto en que termina la relación laboral, la cuenta principal del usuario (como Active Directory o Google Workspace) quede completamente suspendida.

💡 **Diseña una entrevista de salida con enfoque en seguridad:** Aprovecha el último día del colaborador para que firme un documento de "Recordatorio de Obligaciones de Confidencialidad". En este acto, además de recibir los equipos físicos, se le debe leer formalmente que el software, los datos de clientes y la propiedad intelectual que desarrolló pertenecen a la empresa y que su divulgación posterior conlleva consecuencias legales penales.

💡 **Controla la movilidad interna para evitar el "Monstruo de los Accesos":** Cuando un empleado es promovido o transferido de departamento, tendemos a darle sus nuevos accesos pero olvidamos quitarle los anteriores. Establece como regla estricta que todo cambio de puesto exige una revisión y depuración completa de su perfil de usuario; el acumular privilegios del pasado debilita gravemente tu control de accesos.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el procedimiento formal de baja de personal (Offboarding) y de cambio de funciones, junto con las listas de verificación (check-lists) correspondientes. Para validar su eficacia, seleccionará una muestra de empleados y contratistas que hayan salido de la organización o cambiado de puesto en los últimos meses; acto seguido, contrastará las fechas y horas exactas de sus bajas oficiales (registradas por Recursos Humanos) contra las bitácoras del sistema.



Cláusula 6: Controles de personas

Control 6.6 Acuerdos de confidencialidad o no divulgación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Recursos_humanos_seguridad # Información_protección # relaciones_con_proveedores	# Gobernanza_y_Ecosistema

- **El Control:** Los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben identificarse, revisarse periódicamente y ser firmados por el personal y otras partes interesadas pertinentes.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en formalizar los requisitos legales para la protección del intercambio de información confidencial con empleados, contratistas y socios comerciales. Los puntos clave resumidos son:
 - Requisitos del Acuerdo:** Los acuerdos de confidencialidad deben definir con total claridad qué información se considera confidencial, las condiciones para su manejo, el período de vigencia y las acciones a tomar en caso de una divulgación no autorizada.
 - Revisiones Periódicas:** Las necesidades de protección de la información de una empresa cambian con el tiempo. Por ello, los formatos y cláusulas de los NDAs deben revisarse y actualizarse periódicamente para asegurar que siguen cubriendo las nuevas tecnologías, tipos de datos (como datos biométricos o IA) y normativas legales vigentes.
 - Cobertura Total:** El control exige que todas las partes interesadas relevantes firmen estos acuerdos antes de que se les conceda cualquier tipo de acceso a información que no sea pública.
 - Custodia y Registro:** La organización debe mantener un registro centralizado y seguro de todos los acuerdos firmados, facilitando la verificación rápida de que ningún tercero o colaborador interno esté operando sin un respaldo legal vinculante.



Cláusula 6: Controles de personas

Control 6.6 Acuerdos de confidencialidad o no divulgación

- **Otra Información:** La norma recuerda que un acuerdo de confidencialidad no exime a la organización de implementar controles técnicos (como cifrado o enmascaramiento de datos). El NDA es un control de tipo disuasorio y legal, pero debe trabajar en conjunto con los controles de seguridad lógicos. Asimismo, señala que las obligaciones del acuerdo deben cumplir estrictamente con las leyes locales de contratos del país donde se ejecuten.

💡 **No uses plantillas genéricas de internet:** Un NDA que sirve para una agencia de marketing digital puede ser completamente inútil para una empresa de desarrollo de software o sector salud. Diseña tus acuerdos de confidencialidad a la medida de tu negocio, asegurándote de mapear con precisión qué es "información confidencial" para tu empresa (código fuente, algoritmos, listas de precios, datos médicos, etc.).

💡 **Estandariza el proceso de firmas con herramientas digitales:** Evita la fuga de controles por pérdida de papel. Implementa plataformas de firma electrónica legalmente válidas para el envío, firma y almacenamiento automatizado de los NDAs de tus empleados y proveedores; esto te permitirá tener un repositorio centralizado, indexado y fácilmente auditable.

💡 **Establece alertas de caducidad para contratos con terceros:** Muchos acuerdos con proveedores tienen cláusulas de confidencialidad ligadas a la duración del contrato comercial. Configura alertas tempranas en tu sistema de gestión de contratos para que, meses antes de que un acuerdo expire, el área legal evalúe si es necesario renovar las cláusulas de no divulgación post-contractuales.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la política o el procedimiento que rige el uso de los acuerdos de confidencialidad (NDAs) y los formatos estándar aprobados por el área legal. Para verificar su cumplimiento operacional, seleccionará una muestra aleatoria que incluya tanto a empleados contratados recientemente como a proveedores, consultores externos o partners que tengan acceso a la red o manejen datos de la empresa; el auditor validará visualmente que cada uno de ellos cuente con un acuerdo debidamente firmado y fechado antes del inicio de sus operaciones.



Cláusula 6: Controles de personas

Control 6.7 Trabajo Remoto

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gestión de activos # Information_protec- ción # Seguridad física # sistema_y_red- trabajo_seguridad	# Proteccion

- **El Control:** Se deben implementar medidas de seguridad cuando el personal trabaje a distancia para proteger la información a la que se accede, se procesa o se almacena fuera de las instalaciones de la organización.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en regular y proteger las actividades laborales realizadas fuera de los límites físicos de la oficina corporativa (home office, viajes de negocio, etc.). Los puntos clave resumidos son:
 - Política de Trabajo Remoto:** La organización debe definir una política específica que autorice qué roles pueden trabajar a distancia, las condiciones bajo las cuales se permite y los requisitos técnicos de seguridad obligatorios.
 - Seguridad en el Entorno Físico:** El colaborador es responsable de garantizar que su lugar de trabajo remoto sea seguro. Esto implica evitar que familiares o terceros visualicen pantallas con datos confidenciales (shoulder surfing) y asegurar físicamente los dispositivos contra robo o pérdida.
 - Controles Tecnológicos Básicos:** Se debe exigir el uso de conexiones seguras y cifradas, como Redes Privadas Virtuales (VPN), la implementación de Autenticación de Múltiple Factor (MFA), el uso de antivirus actualizados y el cifrado de los discos duros de los equipos portátiles.
 - Uso de Dispositivos (BYOD vs. Corporativos):** La guía prefiere el uso de equipos propiedad de la empresa. Si se permite que el personal use sus propios dispositivos (Bring Your Own Device - BYOD), se deben aplicar controles estrictos de segregación de datos, como soluciones de Gestión de Dispositivos Móviles (MDM).



Cláusula 6: Controles de personas

Control 6.7 Trabajo Remoto

- **Otra Información:** La norma resalta que el trabajo remoto incrementa significativamente los riesgos de interceptación de comunicaciones (por ejemplo, al usar redes Wi-Fi públicas en cafeterías o aeropuertos). Por ende, se debe concientizar al personal sobre los riesgos de la ingeniería social fuera de la oficina y la importancia de realizar copias de seguridad de la información si esta se almacena localmente.

💡 **MFA y VPN no son negociables:** No permitas que ningún colaborador acceda a la infraestructura de la empresa desde su casa con una simple contraseña. Implementa de forma obligatoria el uso de Autenticación de Múltiple Factor (MFA) combinado con una VPN robusta; este binomio es tu primera y más fuerte línea de defensa contra accesos no autorizados.

💡 **Bloquea los puertos USB y cifra los discos:** Un equipo portátil fuera de la oficina es un blanco fácil para el robo físico o la fuga de información. Utiliza herramientas de configuración centralizada para cifrar por completo el disco duro de las laptops corporativas (como BitLocker o FileVault) y deshabilita la transferencia de archivos hacia memorias USB externas no autorizadas.

💡 **Prohíbe terminantemente el uso de Wi-Fi públicas abiertas:** Educa a tu personal para que entienda que conectarse al Wi-Fi gratuito de una cafetería sin protección es un riesgo crítico de interceptación de datos. Establece en tu política que, si no disponen de una red doméstica segura, utilicen exclusivamente los datos móviles de su teléfono celular corporativo para trabajar.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Trabajo Remoto vigente y la evidencia de su comunicación y aceptación por parte de los empleados. Posteriormente, seleccionará una muestra de usuarios que operen bajo esta modalidad y pedirá demostraciones técnicas en tiempo real: comprobará que las conexiones a la red interna exijan obligatoriamente el uso de VPN y MFA, verificará a través de la consola centralizada (Active Directory o MDM) que los discos duros de los equipos remotos estén efectivamente cifrados, y revisará las configuraciones de seguridad para constatar que los usuarios no tengan privilegios de administrador local que les permitan desactivar el antivirus o instalar software no autorizado.



Cláusula 6: Controles de personas

Control 6.8 Reporte de eventos de seguridad de la información

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

- **El Control:** El personal debe reportar los eventos de seguridad de la información observados o sospechados a través de los canales organizacionales apropiados de manera oportuna.
- **Resumen de las Directrices de Implementación:**La guía de implementación se enfoca en crear un mecanismo ágil para que los colaboradores actúen como la primera línea de detección ante posibles incidentes. Los puntos clave resumidos son:
 - Canales de Reporte Claros:** La organización debe establecer y dar a conocer canales específicos, sencillos y accesibles para reportar eventos de seguridad (por ejemplo, un correo electrónico dedicado, una extensión telefónica de emergencia o un botón de reporte en el cliente de correo).
 - Definición de qué Reportar:** Se debe instruir al personal sobre qué constituye un "evento sospechoso". Esto incluye correos de phishing, pérdida o robo de dispositivos, accesos físicos no autorizados, comportamiento inusual del sistema operativo o contraseñas expuestas.
 - Cultura de No Represalias:** El proceso debe alentar el reporte oportuno. Si un empleado cometió un error (como hacer clic en un enlace malicioso), no debe ocultarlo por miedo a un castigo; un reporte rápido permite al equipo de TI contener la amenaza antes de que se propague.
 - Registro y Retroalimentación:** Todos los reportes recibidos deben registrarse formalmente. Se debe dar un acuse de recibo y retroalimentación al usuario que reportó para mantenerlo involucrado y confirmar que su aportación fue valiosa.



Cláusula 6: Controles de personas

Control 6.8 Reporte de eventos de seguridad de la información

- **Otra Información:** La norma resalta la importancia de diferenciar entre un "evento" (una sospecha o anomalía) y un "incidente" (un evento confirmado que daña la seguridad). Este control se asegura de que los eventos lleguen de inmediato al equipo especializado (como el CSIRT o el administrador de seguridad) para que ellos realicen el triaje y determinen si se debe activar el protocolo formal de gestión de incidentes.

💡 **Integra un botón de reporte de phishing en un clic:** Instala un complemento visible en Outlook/Gmail (ej. PhishAlarm o Report Phishing de Microsoft) para que los usuarios notifiquen correos maliciosos sin tener que redactar mensajes manuales a la mesa de ayuda.

💡 **Promueve una política de reporte libre de castigos:** Si un empleado comete un error, felicítalo por avisar de inmediato en lugar de sancionarlo; el miedo al castigo solo provoca que el personal oculte incidentes críticos.

💡 **Automatiza el acuse de recibo y la clasificación inicial:** Configura respuestas automáticas que confirmen la recepción del reporte con un número de ticket y recomendaciones inmediatas (como desconectar el cable de red o cambiar la contraseña).

💡 **El Enfoque del Auditor (Lo que te van a revisar)** El auditor solicitará el Procedimiento de Notificación y Gestión de Eventos de Seguridad y verificará qué canales de comunicación existen para los empleados. Durante la auditoría, seleccionará una muestra de incidentes o reportes generados por usuarios en la mesa de ayuda/SIEM para constatar los tiempos de respuesta y escalamiento; asimismo, entrevistará a colaboradores aleatorios para comprobar si conocen cómo reportar una sospecha de seguridad y revisará el material de capacitación de inducción y concientización para confirmar que se divulgan estos canales periódicamente.



Cláusula 7: Controles Físicos

Control 7.1 Perímetros de seguridad física

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

- **El Control:** Los perímetros de seguridad física deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en crear barreras físicas escalonadas (estrategia de defensa en profundidad) para impedir el acceso no autorizado a las instalaciones de la organización. Los puntos clave resumidos son:
 - Definición de Perímetros:** La organización debe declarar claramente qué zonas de sus instalaciones requieren protección. Esto incluye desde el límite exterior del edificio (vallas, fachadas) hasta perímetros internos específicos (oficinas corporativas, almacenes de TI).
 - Solidez de las Barreras:** Los perímetros físicos deben ser estructuralmente sólidos para resistir intentos de entrada forzada. Las paredes, techos, puertas y ventanas de las áreas críticas deben contar con materiales y cerraduras adecuadas contra intrusiones.
 - Control de Accesos en el Perímetro:** Cada perímetro debe contar con puntos de acceso controlados (puertas con tarjeta magnética, recepciones con guardias, torniquetes). Las áreas de carga y descarga de mercancías deben estar separadas y controladas para evitar que transportistas o personal externo ingresen directamente a zonas protegidas.
 - Sistemas de Detección:** Se deben integrar elementos de soporte como sistemas de videovigilancia (CCTV), alarmas de detección de intrusos y sistemas de iluminación adecuados para monitorear de forma continua los límites perimetrales.



Cláusula 7: Controles Físicos

Control 7.1 Perímetros de seguridad física

- **Otra Información:** La norma destaca que el diseño de los perímetros físicos debe considerar no solo las amenazas humanas (robos, vandalismo, sabotaje), sino también los riesgos ambientales o desastres naturales de la zona geográfica (inundaciones, incendios, sismos). Asimismo, se aconseja que las áreas altamente confidenciales (como el centro de datos o salas de servidores) no tengan ventanas visibles al público ni señalizaciones exteriores que revelen su función crítica.

💡 **Diseña tu seguridad bajo el concepto de "Capas de Cebolla":** No confíes la seguridad de tus servidores a una sola puerta. Implementa una estrategia de defensa en profundidad donde un atacante deba superar múltiples perímetros sucesivos: la caseta de vigilancia exterior, la recepción del edificio, el control de acceso del piso de TI y, finalmente, la autenticación biométrica del centro de datos.

💡 **Ocultas tus activos más valiosos de la vista pública:** La discreción es un control de seguridad sumamente efectivo y de bajo costo. Evita colocar letreros llamativos que digan "Sala de Servidores Principal" o "Centro de Monitoreo de Seguridad", y asegúrate de que las ventanas de las oficinas que albergan información confidencial cuenten con películas de privacidad o persianas cerradas para mitigar el espionaje visual.

💡 **Controla estrictamente las zonas de carga y descarga:** Los muelles de recepción de mercancías y mensajería suelen ser el punto más débil del perímetro físico porque entra y sale personal ajeno a la empresa constantemente. Aísla estas áreas mediante puertas intermedias cerradas, asegurando que los repartidores permanezcan en una zona de espera controlada y nunca tengan paso libre hacia los pasillos internos de la organización.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará los planos de distribución física de las instalaciones o el plano de zonificación de seguridad para constatar que los perímetros críticos han sido formalmente identificados y clasificados por niveles de riesgo. Posteriormente, realizará un recorrido físico por las instalaciones (walkthrough) para inspeccionar visualmente la solidez de las barreras estructurales.



Cláusula 7: Controles Físicos

Control 7.2 Entrada física

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Identity_and_Ac- cess_Management	# Proteccion

- **El Control:** Las áreas seguras deben estar protegidas por controles de acceso adecuados para garantizar que solo se permita el acceso al personal autorizado.
 - **Resumen de las Directrices de Implementación:** La guía de implementación detalla los mecanismos operativos y tecnológicos necesarios para gestionar, registrar y autorizar el paso de personas a través de los **perímetros definidos**. Los puntos clave resumidos son:
 - Autenticación e Identificación:** Se deben utilizar dispositivos de control de acceso físico (tarjetas magnéticas, llaves electrónicas, sistemas biométricos o códigos PIN) que permitan identificar de forma inequívoca a cada individuo. El personal debe portar identificaciones visibles en todo momento.
 - Registro de Accesos (Pistas de Auditoría):** Todos los accesos a las áreas seguras deben quedar registrados de forma electrónica (fecha, hora, identidad y sentido del paso). Estas bitácoras deben ser protegidas contra modificaciones y revisarse periódicamente.
- Control de Visitantes y Terceros: Los visitantes externos deben ser registrados a su llegada, verificar su identidad, emitirles una credencial temporal distintiva y permanecer bajo la supervisión de un escolta/acompañante interno autorizado durante toda su estancia. No se les debe permitir el acceso libre.
- Restricción de Derechos de Acceso:** Los derechos de acceso físico deben otorgarse basándose en el rol y la necesidad del negocio. Deben ser revocados de inmediato cuando el colaborador cambie de funciones o termine su relación laboral con la organización.



Cláusula 7: Controles Físicos

Control 7.2 Entrada física

- **Otra Información:** La norma hace una advertencia especial sobre las técnicas de ingeniería social aplicadas al entorno físico, específicamente el tailgating o piggybacking (cuando una persona no autorizada aprovecha la apertura de una puerta por alguien autorizado para colarse detrás). Se recomienda el uso de esclusas de seguridad (mantrap), torniquetes de altura completa o la concientización del personal para mitigar este riesgo.

💡 **Combina la biometría con la videovigilancia en zonas críticas:** Para las áreas de más alto riesgo, como el SITE de telecomunicaciones o la bóveda de respaldos, no te fíes únicamente de las tarjetas de proximidad (que pueden ser clonadas, prestadas o robadas). Implementa lectores biométricos de huella o reconocimiento facial combinados con una cámara de CCTV que apunte directamente al lector para cruzar datos lógicos con evidencia visual.

💡 **Audita las bitácoras de acceso de manera proactiva:** Establece una rutina mensual para auditar los reportes del sistema en busca de anomalías, como intentos de acceso de personal en horarios no laborales, uso de tarjetas que pertenecen a ex-empleados o accesos denegados repetitivos en zonas restringidas.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la política o procedimiento de control de acceso físico y el listado actualizado de personas autorizadas para ingresar a las áreas críticas (como el centro de cómputo o el archivo confidencial). Posteriormente, durante la auditoría in situ, seleccionará una muestra de registros del sistema de control de acceso electrónico correspondientes a días aleatorios y verificará que coincidan con las personas autorizadas en la lista; asimismo, revisará el libro de registro de visitantes externos para confirmar que se capturen sus datos completos y firmas, inspeccionará visualmente que el personal porte sus credenciales en un recorrido físico y solicitará evidencia de que los accesos físicos de los empleados dados de baja recientemente fueron revocados de manera inmediata en la plataforma central de seguridad corporativa.



Cláusula 7: Controles Físicos

Control 7.3 Aseguramiento de oficinas, salas e instalaciones

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

- **El Control:** Se debe diseñar e implementar la seguridad física para oficinas, salas e instalaciones.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en las medidas internas de protección que se deben adoptar dentro de los edificios para evitar el espionaje, el acceso oportunista o el daño a los activos de información. Los puntos clave resumidos son:
 - Estructura Interna Segura:** Las salas que albergan información o infraestructura crítica (como servidores, conmutadores, o el archivo central) deben tener paredes, pisos y techos con resistencia adecuada contra incendios, intrusiones forzadas y daños ambientales.
 - Política de Puertas Cerradas:** Las puertas de acceso a oficinas confidenciales, salas de servidores y centros de procesamiento de datos deben permanecer cerradas con llave o llave electrónica cuando no estén ocupadas, evitando que queden desatendidas.
 - Señalización y Discreción:** Se debe evitar el uso de directorios públicos o señalizaciones externas llamativas que indiquen claramente la ubicación de áreas de procesamiento de datos altamente confidenciales.
 - Prevención de Riesgos de Seguridad y Salud:** Las instalaciones deben contar con sistemas adecuados de control ambiental (aire acondicionado, extracción), detección y supresión de incendios (extintores, rociadores de gas inerte) y sistemas de energía ininterrumpida (UPS) para proteger los equipos críticos.



Cláusula 7: Controles Físicos

Control 7.3 Aseguramiento de oficinas, salas e instalaciones

- **Otra Información:** La norma resalta que se debe considerar la segregación de funciones físicas; por ejemplo, el personal de limpieza, mantenimiento o contratistas externos de infraestructura eléctrica debe ingresar a las salas críticas únicamente bajo supervisión autorizada y en horarios controlados. Asimismo, se aconseja regular el uso de dispositivos de captura de imágenes (como teléfonos inteligentes o cámaras) dentro de estas instalaciones seguras para prevenir fugas de información

💡 **Establece la regla de oro:** "La última persona en salir cierra con llave": Por muy avanzado que sea tu sistema de control de acceso, si los empleados dejan la puerta de una oficina con información confidencial abierta o "con el pestillo puesto" para ir a comer, el control queda anulado. Automatiza este proceso instalando cierrapuertas hidráulicos (brazos mecánicos) en todas las salas críticas para garantizar que la puerta regrese a su posición de bloqueo de forma obligatoria tras cada paso.

💡 **Monitorea los sistemas de soporte tanto como la red:** Asegurar una sala no es solo ponerle candado. Instala sensores de temperatura, humedad y fluidos conectados a un sistema de alerta temprana en tu SITE de telecomunicaciones; un fallo en el aire acondicionado o una pequeña filtración de agua en el techo pueden destruir tus servidores y bases de datos con la misma efectividad que un ciberataque.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor inspeccionará físicamente el diseño constructivo y las medidas de protección interna de las salas seguras y oficinas de la organización. Durante su recorrido, revisará que las puertas de las áreas de TI, archivos físicos y salas de servidores cuenten con chapas de seguridad funcionales y se mantengan cerradas; además, solicitará evidencias de las pruebas de mantenimiento de los sistemas de soporte críticos (mantenimiento de UPS, plantas de luz y recarga de extintores o sistemas de gas de supresión de fuego) y verificará que los registros de acceso físico incluyan los folios de supervisión o autorización asignados al personal de limpieza y proveedores de mantenimiento técnico externo.



Cláusula 7: Controles Físicos

Control 7.4 Supervisión de la seguridad física

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Detectar	# Seguridad física	# Proteccion # Defensa

- **El Control:** Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.
- **Resumen de las Directrices de Implementación:** La guía de implementación se centra en la capacidad de la organización para detectar, alertar y reaccionar ante intrusiones o anomalías físicas en tiempo real. Los puntos clave resumidos son:
 - Sistemas de Monitoreo Continuo:** Se deben emplear sistemas tecnológicos que operen las 24 horas del día, los 7 días de la semana (24/7). Esto incluye Sistemas de Circuitos Cerrados de Televisión (CCTV), detectores de movimiento, sensores de rotura de cristales y sistemas de alarma perimetral.
 - Supervisión y Gestión de Alertas:** De nada sirve acumular video si nadie lo ve. Las alarmas y señales de video deben ser supervisadas activamente por personal dedicado (como un centro de monitoreo de seguridad física o guardias de seguridad) o conectadas a una central de respuesta externa.
 - Mantenimiento y Protección de Bitácoras:** Las grabaciones de las cámaras de seguridad y las bitácoras de los sistemas de alarma deben ser almacenadas de forma segura y protegidas contra el borrado o la manipulación no autorizada.
 - Pruebas Periódicas:** El equipamiento de monitoreo físico debe someterse a pruebas de funcionamiento y mantenimiento de manera regular para asegurar que las cámaras graben con la calidad adecuada, los sensores se disparen correctamente y las alertas lleguen al personal indicado.



Cláusula 7: Controles Físicos

Control 7.4 Supervisión de la seguridad física

- **Otra Información:** La norma resalta la importancia de la convergencia entre la seguridad física y la lógica (ciberseguridad). Por ejemplo, si un sistema de monitoreo de CCTV detecta un acceso inusual fuera de horario a una oficina crítica, esta alerta debería poder correlacionarse con los accesos lógicos a la red de esa misma área, permitiendo identificar ataques combinados o fugas de información internas de manera inmediata.

💡 **No dejes las cámaras a ciegas en la oscuridad:** Un error común es instalar sistemas de CCTV de alta definición pero olvidar que los delincuentes prefieren actuar de noche. Asegúrate de que las cámaras perimetrales y las que apuntan a áreas críticas (como el SITE o archivos confidenciales) tengan capacidades de visión nocturna (infrarrojos) o estén respaldadas por sistemas de iluminación con sensores de movimiento que se activen automáticamente ante cualquier presencia.

💡 **Proteja el grabador (NVR/DVR) como si fuera oro:** El grabador de tus cámaras debe estar estrictamente resguardado dentro de un rack cerrado con llave, dentro de una sala segura con control de acceso restrictivo, o idealmente, replicando los videos críticos en la nube de forma cifrada.

💡 **Establece un protocolo claro de reacción ante alarmas:** Diseña una matriz de escalación clara y entrena a tus guardias o proveedores de monitoreo para que sepan exactamente qué hacer: desde realizar una verificación visual remota instantánea, hasta dar aviso inmediato a la policía local o al equipo de respuesta a incidentes de la empresa.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el inventario y planos de ubicación de los sistemas de monitoreo físico (CCTV y alarmas) junto con las bitácoras de pruebas y mantenimiento preventivo de dichos equipos. Durante la auditoría, pedirá que se le muestre en vivo el centro de control o las pantallas de monitoreo, validará que las cámaras seleccionadas en la muestra tengan la cobertura y resolución adecuadas sin puntos ciegos críticos, revisará que el almacenamiento de video cumpla con los días de retención estipulados en la política y solicitará evidencia del último reporte de incidentes físicos o falsas alarmas para comprobar que se sigue un protocolo formal de atención y escalación de eventos sospechosos.



Cláusula 7: Controles Físicos

Control 7.5 Protección contra amenazas físicas y ambientales

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física	# Protección

- **El Control:** Se debe diseñar e implementar protección contra amenazas físicas y ambientales, tales como incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o provocados por el hombre.
- **Resumen de las Directrices de Implementación:** La guía de implementación busca evitar que factores externos o de la naturaleza destruyan el hardware, los archivos físicos o interrumpen la disponibilidad de los servicios críticos de la organización. Los puntos clave resumidos son:
 - Evaluación de Riesgos Geográficos:** La organización debe identificar a qué amenazas está expuesta según su ubicación (zonas sísmicas, áreas propensas a inundaciones, cercanía a plantas químicas o zonas de alta conflictividad social) y diseñar las instalaciones con base en ello.
 - Protección contra Incendios:** Se deben instalar sistemas automáticos de detección de humo y calor, combinados con sistemas de supresión de incendios adecuados para entornos tecnológicos (como gas inerte o agentes limpios), evitando el uso de agua que dañaría irreversiblemente los servidores.
 - Protección contra Agua e Inundaciones:** Los centros de datos o SITEs de telecomunicaciones no deben ubicarse en sótanos si existe riesgo de inundación, ni debajo de tuberías de agua o sistemas de aire acondicionado propensos a fugas. Se recomienda el uso de sensores de líquido en el suelo.
 - Resiliencia Estructural y Eléctrica:** Los edificios deben cumplir con normas de construcción antisísmicas y contar con pararrayos. Asimismo, los sistemas críticos deben estar protegidos contra fallos de energía mediante Sistemas de Energía Ininterrumpida (UPS) y plantas de luz (generadores diésel) con suficiente combustible.



Cláusula 7: Controles Físicos

Control 7.5 Protección contra amenazas físicas y ambientales

- **Otra Información:** La norma aconseja que los materiales utilizados en la construcción de salas seguras sean ignífugos (resistentes al fuego) y que los consumibles peligrosos o inflamables se almacenen de forma aislada y a una distancia segura del edificio principal.

💡 **El agua es el enemigo silencioso de los servidores:** Cuando pensamos en desastres en el SITE, usualmente imaginamos un incendio, pero las filtraciones de agua por aires acondicionados defectuosos o tuberías ocultas son mucho más comunes. Instala cables sensores de inundación perimetrales debajo del falso piso de tu centro de datos para recibir alertas tempranas antes de que el agua toque tus racks.

💡 **Prueba tus plantas de luz con "carga real":** Tener un generador diésel costoso no garantiza que funcionará durante un apagón masivo si solo lo enciendes en vacío (sin conectar los servidores) durante tus pruebas mensuales. Programa ventanas de mantenimiento anuales para transferir la carga real de la empresa a la planta de luz y verificar que aguanta la demanda operativa sin caídas de tensión.

💡 **Capacita al personal en el uso de los sistemas de supresión:** Instalar costosos sistemas de gas inerte (como FM-200 o Novec) no sirve si los empleados entran en pánico ante una alarma y abren las puertas de la sala, disipando el gas y permitiendo que el fuego continúe. Asegúrate de que el equipo de TI y brigadistas conozcan los tiempos de descarga, los botones de aborto manual y los protocolos de evacuación segura.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la matriz de riesgos ambientales que justifique las medidas de diseño de la infraestructura, así como los contratos de mantenimiento, bitácoras de pruebas y certificados de recarga de los sistemas de detección/supresión de incendios y plantas de emergencia. Durante la revisión física, inspeccionará las condiciones del SITE de telecomunicaciones para verificar que no pasen tuberías de agua vivas sobre los racks, comprobará la ubicación y fecha de vigencia de los extintores, revisará el nivel de combustible del generador y pedirá los registros que demuestren que los sistemas de respaldo eléctrico (UPS) son capaces de soportar la operación mientras la planta de luz



Cláusula 7: Controles Físicos

Control 7.6 Trabajar en áreas seguras

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

- **El Control:** El personal debe trabajar en áreas seguras solo cuando sea necesario y sus actividades deben ser monitoreadas.
- **Resumen de las Directrices de Implementación:** La guía de implementación regula el comportamiento, las buenas prácticas y las restricciones que el personal (interno o externo) debe seguir cuando realiza sus labores diarias dentro de las zonas consideradas de alta seguridad. Los puntos clave resumidos son:
 - Necesidad de Acceso (Justificación):** El personal no debe permanecer en áreas seguras (como centros de datos, bóvedas o salas de control) por comodidad o rutina; el acceso y la estancia deben limitarse estrictamente a cuando la función laboral lo requiera.
 - Restricción de Dispositivos de Captura:** Se debe prohibir o controlar estrictamente la introducción de dispositivos capaces de grabar imágenes, video o audio (como teléfonos inteligentes, tabletas o cámaras fotográficas) para evitar el espionaje industrial o la fuga de datos visuales.
 - Supervisión de Actividades:** Las actividades realizadas dentro de las áreas seguras deben ser monitoreadas, ya sea mediante la supervisión visual directa de un colega o supervisor, o mediante el uso continuo de sistemas de videovigilancia (CCTV) sin puntos ciegos.
 - Reglas de Comportamiento e Higiene:** Se debe prohibir el consumo de alimentos y bebidas dentro de áreas técnicas críticas para evitar daños accidentales a los equipos. Asimismo, las áreas de trabajo deben mantenerse despejadas y libres de documentos confidenciales expuestos.



Cláusula 7: Controles Físicos

Control 7.6 Trabajar en áreas seguras

- **Otra Información:** La norma resalta que se debe considerar la seguridad del personal que trabaja en estas áreas, especialmente si laboran de manera aislada (trabajadores en solitario o lone workers). En estos casos, se deben implementar mecanismos de alerta o botones de pánico. También se menciona que los horarios de trabajo dentro de estas zonas deben estar predefinidos y cualquier actividad fuera de horas laborables requiere una autorización especial por escrito.

💡 **Establece la regla de "Cero Comida y Bebida" de forma estricta:** Un café derramado sobre un teclado en una oficina común es un accidente menor, pero un vaso de agua vertido sobre un conmutador o servidor central en el SITE puede detener la operación de toda la empresa. Coloca señalizaciones claras y botes de basura fuera de las áreas seguras para que nadie ingrese con alimentos bajo ninguna circunstancia.

💡 **Controla el uso de smartphones en zonas de alta confidencialidad:** Si tienes áreas donde se procesa propiedad intelectual, datos bancarios o servidores críticos, implementa casilleros seguros en la entrada para que el personal deposite sus dispositivos móviles antes de ingresar a laborar.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará las reglas de conducta escritas y las políticas específicas para el trabajo dentro de áreas seguras, así como la evidencia de que estas han sido comunicadas al personal y contratistas. Durante la inspección física de las zonas restringidas, el auditor verificará visualmente la existencia de señalizaciones de prohibición (como restricciones de alimentos o uso de cámaras), revisará si existen casilleros para resguardo de celulares si la política lo exige, y comprobará que las cámaras de CCTV estén posicionadas de tal manera que puedan registrar las actividades de mantenimiento en los pasillos de los racks; finalmente, pedirá revisar las bitácoras de acceso fuera de horario para confirmar que cada entrada nocturna o de fin de semana contó con una justificación y autorización formal.



Cláusula 7: Controles Físicos

Control 7.7 Escritorio despejado y pantalla despejada

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Seguridad física	# Proteccion

- **El Control:** Se debe adoptar una política de escritorio despejado para documentos y medios de almacenamiento extraíbles, y una política de pantalla despejada para las instalaciones de procesamiento de información.
- **Resumen de las Directrices de Implementación:** La guía de implementación busca reducir el riesgo de acceso no autorizado, pérdida o daño de la información expuesta a la vista en el día a día laboral. Los puntos clave resumidos son:
 - Escritorio Despejado (Clear Desk):** Los documentos impresos, expedientes, notas adhesivas (post-its) con contraseñas y medios de almacenamiento removibles (USB, discos duros externos) no deben dejarse desatendidos en los escritorios, especialmente cuando el personal se ausenta de su lugar o al finalizar la jornada.
 - Pantalla Despejada (Clear Screen):** Se debe configurar un bloqueo automático por inactividad tras un período corto de tiempo (por ejemplo, de 3 a 5 minutos).
 - Protección en la Impresión:** Los documentos impresos confidenciales o clasificados deben ser retirados de las impresoras, copiadoras o faxes corporativos inmediatamente después de ser procesados para evitar que terceros los recojan o visualicen por error.
 - Medios de Desecho Seguro:** Toda información impresa que ya no sea necesaria debe destruirse .



Cláusula 7: Controles Físicos

Control 7.7 Escritorio despejado y pantalla despejada

- **Otra Información:** La norma resalta que este control es especialmente relevante en áreas de atención al público, recepciones y en entornos de oficinas abiertas o espacios de co-working, donde el flujo de personas ajenas a la organización es constante. También destaca que la política debe aplicar de igual manera al entorno de trabajo remoto (home office) para salvaguardar la privacidad de la información frente a familiares o visitas.

💡 **Automatiza el bloqueo de pantalla por directiva de grupo:** No dejes la seguridad en manos de la memoria de tus empleados. Configura una directiva centralizada (GPO o MDM) que bloquee las estaciones de trabajo automáticamente tras un máximo de 5 minutos de inactividad; para rematar, acostumbra a tu personal a utilizar el atajo de teclado definitivo: la tecla Windows + L cada vez que se levanten por un café.

💡 **Implementa impresión segura por PIN o credencial:** El eslabón perdido del "clear desk" suele ser la bandeja de salida de la impresora común, donde se acumulan estados financieros o nóminas que nadie recoge. Adopta soluciones de impresión retenida (Pull Printing), donde el documento solo se imprime físicamente cuando el usuario se presenta ante la máquina y pasa su credencial corporativa o digita su código PIN personal.

💡 **Erradica el peligro de los post-its con contraseñas:** Realiza campañas periódicas de concienciación y "limpieza" en las oficinas. El hábito de pegar las contraseñas en el monitor o debajo del teclado destruye cualquier control lógico; dótales en su lugar de un gestor de contraseñas corporativo homologado que les permita almacenar sus accesos de forma segura y cifrada.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política formal de Escritorio Despejado y Pantalla Despejada y verificará su correcta difusión en la empresa. Posteriormente, el auditor realizará inspecciones visuales sin previo aviso en las áreas de trabajo (incluso fuera del horario laboral o durante la hora del almuerzo) para comprobar que no existan documentos confidenciales o tokens USB desatendidos sobre los escritorios; asimismo, observará que las pantallas de los usuarios ausentes estén bloqueadas, revisará las configuraciones del sistema para validar el tiempo asignado al bloqueo automático por inactividad y visitará las islas de impresión comunes para constatar que no haya documentos olvidados en las bandejas.



Cláusula 7: Controles Físicos

Control 7.8 Ubicación y protección del equipo

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

- **El Control:** El equipo debe ubicarse y protegerse para reducir los riesgos derivados de las amenazas y peligros ambientales, así como las oportunidades de acceso no autorizado.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en la disposición física estratégica del hardware (servidores, estaciones de trabajo, almacenamiento) para minimizar su exposición a daños o manipulaciones. Los puntos clave resumidos son:
 - Ubicación Estratégica:** Los equipos que procesan o almacenan información crítica deben colocarse en lugares que minimicen el tránsito de personas. Las pantallas que muestran datos confidenciales deben orientarse de tal forma que no puedan ser vistas por personas no autorizadas desde pasillos o ventanas (shoulder surfing).
 - Protección Contra Factores Ambientales:** El hardware debe estar resguardado de fuentes de peligro físico directo. Esto implica mantenerlo alejado de ventanas (riesgo de rotura, lluvia o radiación solar directa), de tuberías de agua o gas, y de áreas de almacenamiento de químicos o materiales inflamables.
 - Aislamiento de Equipos Críticos:** Los servidores, equipos de red (switches, routers) y consolas de administración central deben estar alojados preferentemente en gabinetes (racks) cerrados con llave, dentro de salas dedicadas con acceso restringido.
 - Controles para Equipamiento Especial:** Se deben aplicar medidas adicionales a los equipos instalados en áreas industriales, plantas de manufactura o exteriores, tales como el uso de carcasas de protección industrial contra polvo, vibraciones extremas o interferencia electromagnética.



Cláusula 7: Controles Físicos

Control 7.8 Ubicación y protección del equipo

- **Otra Información:** La norma también advierte sobre los riesgos asociados a los cables de red y de alimentación eléctrica. Recomendamos que el cableado de datos y de energía esté canalizado mediante canaletas ocultas o tubos de protección (conduit) para evitar daños accidentales, cortes del servicio o interceptaciones de señal por parte de atacantes físicos.

💡 **Utiliza micas de privacidad para pantallas expuestas:** No todas las oficinas pueden estar aisladas del público. Si tienes personal en recepción, áreas de atención a clientes o ventanillas financieras que manejan datos personales, instala micas de privacidad físicas en sus monitores; estas micas oscurecen por completo la pantalla si alguien intenta mirar desde un ángulo lateral, anulando el espionaje visual.

💡 **Protege tus cables de red y energía de los tropiezos:** Un cable suelto debajo de un escritorio o cruzando un pasillo no solo es un riesgo de seguridad laboral, sino un incidente de disponibilidad en potencia. Asegúrate de que todo el cableado estructural y de energía esté firmemente canalizado y etiquetado; un tirón accidental al mover una silla puede desconectar un equipo crítico en el momento menos oportuno.

💡 **Aísla las consolas de control industrial (OT):** Coloca estas estaciones de trabajo dentro de quioscos cerrados de grado industrial que requieran autenticación y que protejan los puertos USB físicos contra la introducción de malware.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor realizará una inspección ocular detallada de la distribución física de los equipos en las oficinas y el centro de datos de la organización. Durante el recorrido, verificará que las pantallas de los usuarios no sean visibles desde las áreas de tránsito público, comprobará que los switches de red y paneles de parcheo (patch panels) periféricos ubicados en los pasillos estén resguardados en gabinetes cerrados bajo llave, e inspeccionará que los servidores e infraestructura crítica del SITE no colinden directamente con muros exteriores vulnerables o tuberías de agua expuestas que pongan en riesgo la integridad física del hardware.



Cláusula 7: Controles Físicos

Control 7.9 Seguridad de los activos fuera de las instalaciones

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

- **El Control:** Los activos fuera de las instalaciones deben ser protegidos.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en resguardar los equipos portátiles, dispositivos móviles y cualquier activo de información de la empresa cuando son trasladados o utilizados fuera del perímetro físico de la organización (por ejemplo, en viajes de negocio, home office, o eventos externos). Los puntos clave resumidos son:
 - Autorización de Salida:** Ningún activo de la empresa debe salir de las instalaciones sin una autorización previa y documentada. Se debe mantener un registro (inventario) de qué equipos están fuera, quién es el responsable y cuándo se prevé su retorno.
 - Protección Física Durante el Traslado:** Los usuarios deben ser responsables de la custodia física de los equipos. Se deben evitar conductas de riesgo, como dejar computadoras portátiles a la vista dentro de un automóvil estacionado o desatendidas en salas de espera de aeropuertos y hoteles.
 - Seguridad en el Almacenamiento Externo:** Si los activos deben guardarse en un sitio ajeno a la organización (como el hogar del empleado o instalaciones de un cliente), se deben verificar las condiciones de seguridad física del lugar para mitigar riesgos de robo o daños por factores ambientales.
 - Seguro de Activos:** Cuando sea financieramente viable y el nivel de riesgo lo amerite, la organización debe considerar la contratación de pólizas de seguro específicas que cubran el robo, pérdida o daño de los equipos asignados al personal móvil.



Cláusula 7: Controles Físicos

Control 7.9 Seguridad de los activos fuera de las instalaciones

- **Otra Información:** La norma resalta que, debido a que el entorno fuera de las instalaciones no puede ser controlado al 100% por la empresa, los controles físicos de este apartado deben depender fuertemente de controles lógicos complementarios. Si un activo físico se pierde, el impacto de seguridad se neutraliza casi por completo si los datos internos están adecuadamente cifrados y si el equipo cuenta con capacidades de rastreo y borrado remoto de la información.



Crea una política estricta para el "Auto como Oficina": El escenario de robo más común ocurre cuando un colaborador deja la mochila de la laptop en el asiento trasero de su vehículo mientras entra a un restaurante o gasolinera. Prohíbe explícitamente en tus políticas dejar equipos visibles en los automóviles y capacita al personal para que, si es estrictamente necesario dejarlos en el vehículo, los resguarden en la cajuela antes de llegar a su destino.



Digitaliza el pase de salida de activos: Olvídate de las hojas de papel firmadas a mano que se terminan perdiendo en una carpeta de vigilancia. Implementa un sistema digital de pases de salida (puede ser mediante un flujo sencillo de Service Desk o software de inventarios) donde el empleado solicite la salida del equipo, su jefe autorice y el guardia de seguridad pueda escanear un código QR al momento de la salida física.



Vincula este control con herramientas de borrado remoto (MDM): Asegúrate de que todas las laptops y smartphones corporativos estén enrolados en un sistema de Gestión de Dispositivos Móviles (MDM); si el empleado reporta el robo de su equipo en un viaje, el equipo de TI debe ser capaz de ejecutar un comando de "Wipe" (borrado de fábrica) en cuestión de segundos.



El Enfoque del Auditor (Lo que te van a revisar): El auditor solicitará el procedimiento de autorización para la salida de activos y la política de responsabilidades de los usuarios para equipos portátiles. Para validar su cumplimiento, cruzará el inventario general de hardware contra el registro de pases de salida vigentes; asimismo, seleccionará una muestra de colaboradores asignados a modalidades remotas o comerciales y pedirá los acuses de recibo firmados donde aceptan las condiciones de seguridad para el resguardo de los equipos fuera de las instalaciones.



Cláusula 7: Controles Físicos

Control 7.10 Medios de almacenamiento

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

- **El Control:** Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación, de acuerdo con el esquema de clasificación y los requisitos de manejo de la organización.
- **Resumen de las Directrices de Implementación:** La guía de implementación busca proteger los datos confidenciales contenidos en cualquier soporte físico de almacenamiento (discos duros, SSD, cintas de respaldo, memorias USB, tarjetas SD e incluso documentos impresos):
 - Gestión del Ciclo de Vida:** Se deben establecer procedimientos para todas las etapas del medio: adquisición segura, uso controlado, transporte protegido y disposición final o destrucción.
 - Control de Uso y Acceso:** Los medios de almacenamiento que contengan información sensible deben ser inventariados, etiquetados según su nivel de clasificación (ej. Confidencial) y almacenados en lugares seguros bajo llave cuando no se utilicen.
 - Transporte Seguro:** Si es necesario trasladar medios físicos con datos fuera de las instalaciones (como cintas de respaldo a un sitio alternativo), se deben usar mensajerías confiables, contenedores resistentes con candados o sellos de seguridad y, de forma obligatoria, los datos deben estar cifrados.
 - Eliminación y Destrucción Segura:** Cuando un medio de almacenamiento cumple su vida útil o va a ser reutilizado, los datos deben ser borrados de forma segura mediante desmagnetización (degaussing), sobreescritura con software certificado, o destrucción física destructiva (trituration) para evitar la recuperación de remanentes de información.



Cláusula 7: Controles Físicos

Control 7.10 Medios de almacenamiento

- **Otra Información:** La norma enfatiza que el simple comando de "borrar" o "formatear" un sistema operativo no elimina los datos de forma permanente, por lo que se requiere software especializado de borrado seguro o destrucción física. Además, advierte que los dispositivos multifuncionales modernos (como impresoras y copiadoras corporativas) contienen discos duros internos que almacenan copias de los documentos procesados, los cuales también deben ser purgados antes de devolver o desechar los equipos.



Prohíbe las memorias USB genéricas y no cifradas: Las unidades USB son el vector perfecto para la fuga de datos y la entrada de malware. Implementa una política estricta donde solo se permita el uso de memorias USB corporativas que cuenten con cifrado por hardware obligatorio y bloquea mediante software el uso de cualquier dispositivo de almacenamiento externo que no esté autorizado en el inventario de TI.



Exige certificados de destrucción a tus proveedores: Contrata a una empresa externa certificada en la destrucción segura de activos tecnológicos que te entregue un reporte detallado con los números de serie de cada disco destruido y un certificado de destrucción digital avalado bajo estándares internacionales (como NIST SP 800-88).



Aplica el cifrado total en el transporte de respaldos: Si todavía utilizas esquemas híbridos que involucran mover cintas físicas o discos duros externos para resguardo fuera de sitio (off-site backup), la regla de oro es que el 100% de los datos grabados en esos medios deben estar cifrados antes de salir del SITE; si el transportista pierde el portafolios, el impacto reputacional y legal será nulo porque la información será totalmente ilegible.



El Enfoque del Auditor (Lo que te van a revisar): El auditor solicitará el procedimiento de gestión de medios de almacenamiento y las políticas de destrucción segura de la información. Para comprobar su cumplimiento, revisará el inventario de activos lógicos, seleccionará una muestra de equipos de cómputo dados de baja o devueltos por los usuarios en el último año y pedirá evidencia documental que demuestre que el almacenamiento interno fue purgado de manera irreversible; adicionalmente, verificará visualmente las condiciones de almacenamiento y custodia de los medios que contienen respaldos activos dentro de las instalaciones.



Cláusula 7: Controles Físicos

Control 7.11 Utilidades de apoyo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Integridad # Disponibilidad	# Proteger #Detectar	# Seguridad física	# Proteccion

- 💡 **El Control:** Las instalaciones que contienen servicios de procesamiento de información deben estar protegidas contra fallos de energía y otras interrupciones causadas por fallos en las utilidades de apoyo.
- Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en garantizar la continuidad operativa y la disponibilidad de la infraestructura tecnológica mediante el suministro estable de servicios básicos o utilidades (energía eléctrica, agua, telecomunicaciones, aire acondicionado, gas, etc.). Los puntos clave resumidos son:
 - Suministro Eléctrico Continuo:** Las instalaciones críticas deben contar con Sistemas de Energía Ininterrumpida (UPS) de capacidad adecuada para absorber variaciones de voltaje y mantener los equipos encendidos mientras entra en operación una fuente secundaria, como una planta de luz (generador diésel).
 - Control Ambiental (Climatización):** Los centros de datos y salas de cableado (SITEs) requieren sistemas de aire acondicionado de precisión que mantengan la temperatura y humedad dentro de los rangos recomendados por los fabricantes para evitar sobrecalentamientos o estática.
 - Redundancia en Telecomunicaciones:** Se deben contratar múltiples proveedores de servicios de internet y enlaces de datos (enlaces redundantes) ingresando al edificio por rutas físicas distintas para evitar que un corte de cableado externo deje a la organización incomunicada.
 - Mantenimiento Preventivo:** Todos los sistemas de apoyo (UPS, generadores, aires acondicionados) deben estar sujetos a un estricto programa de mantenimiento periódico y pruebas de funcionamiento bajo carga para asegurar su respuesta ante una emergencia real.



Cláusula 7: Controles Físicos

Control 7.11 Utilidades de apoyo

- **Otra Información:** La norma resalta que los puntos de suministro y las conexiones de estas utilidades (como los medidores de luz, las cisternas de agua, las plantas de emergencia o las cajas de distribución de telefonía) deben estar físicamente protegidos y cerrados con llave para evitar el acceso de personal no autorizado, vandalismo o sabotaje.

💡 **Evita el "punto único de fallo" en tu conectividad:** De nada sirve tener dos proveedores de internet si los cables de fibra óptica de ambas compañías entran al edificio por el mismo tubo plástico (ducto). Asegúrate de que tus enlaces de respaldo tengan redundancia geográfica real, ingresando por fachadas u orientaciones distintas de tus instalaciones para que una excavación accidental en la calle no rompa ambas conexiones a la vez.

💡 **Automatiza las alertas de climatización de tus SITES:** Las fallas en los aires acondicionados ocurren cuando nadie está mirando, por lo general en fines de semana o madrugadas. Configura sensores ambientales IP que envíen alertas automáticas (vía SMS, correo o herramientas de mensajería como Teams/Slack) de inmediato al equipo de TI en cuanto la temperatura del cuarto de servidores supere los 24°C, permitiendo una acción rápida antes de que los equipos se apaguen por seguridad.

💡 **Monitorea los niveles y calidad del combustible del generador:** Mantén el tanque a un mínimo del 75% de su capacidad, realiza pruebas de arranque mensuales y contrata anualmente un servicio de filtrado ("pulido") del diésel para garantizar que los motores arranquen al primer intento ante un apagón.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará los contratos de mantenimiento, bitácoras de servicio y reportes de pruebas de los sistemas de soporte críticos (UPS, generadores eléctricos y sistemas de aire acondicionado). Para validar la efectividad de este control, inspeccionará físicamente el resguardo y protección de las áreas donde se ubican las plantas de luz y subestaciones, verificará las alertas históricas del sistema de monitoreo ambiental y requerirá evidencias de los simulacros de transferencia de energía.



Cláusula 7: Controles Físicos

Control 7.12 Seguridad del cableado

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

- **El Control:** El cableado que transporta energía o datos, o que soporta servicios de información, debe protegerse contra la interceptación, la interferencia o el daño.
- **Resumen de las Directrices de Implementación:** La guía de implementación busca resguardar las "arterias" de comunicación y energía de la organización, evitando cortes accidentales, sabotajes o el espionaje mediante la intervención de líneas físicas. Los puntos clave resumidos son:
 - Segregación de Cables:** Las líneas de datos (redes ethernet, fibra óptica) y las líneas de energía eléctrica deben estar físicamente separadas para evitar que la inducción electromagnética de la electricidad corrompa o degrade la velocidad y calidad de la transmisión de datos.
 - Canalización y Blindaje Físico:** El cableado estructural debe correr a través de conductos protegidos, como tuberías rígidas (conduit), canaletas cerradas o por debajo de falso piso/falso techo, bloqueando el acceso visual y físico de personas no autorizadas.
 - Protección de Puntos de Conexión:** Los nodos de red, paneles de parcheo (patch panels) y los armarios de distribución intermedia (IDF/murales) distribuidos en las oficinas deben estar resguardados en gabinetes cerrados bajo llave.
 - Inspecciones Regulares:** Se deben realizar revisiones periódicas de las rutas de cableado y los cuartos de conexiones para detectar posibles modificaciones no autorizadas, cables sueltos, "puentes" sospechosos o daño por desgaste o plagas (roedores).



Cláusula 7: Controles Físicos

Control 7.12 Seguridad del cableado

- **Otra Información:** La norma resalta que, para la transmisión de datos altamente sensibles, se debe priorizar el uso de fibra óptica sobre el cable de cobre (UTP), ya que la fibra es considerablemente más difícil de intervenir de forma clandestina sin interrumpir el servicio y alertar a los administradores. Además, advierte que en las zonas de acceso público (como recepciones o salas de espera), los puertos de red de pared que no estén en uso activo deben deshabilitarse lógicamente desde el switch de TI.

💡 **Apaga los puertos de red "vivos" en zonas comunes:** Un puerto de red ethernet desprotegido en la sala de espera o en una sala de juntas compartida es una invitación abierta para que un atacante conecte una laptop y acceda a tu red interna. Establece la política estricta de desactivar de forma lógica en el switch (shut down) cualquier nodo físico de pared que no esté asignado a un equipo corporativo fijo.

💡 **Respeta las distancias normadas entre luz y datos:** Exige que se mantenga una distancia mínima de separación (generalmente de 20 a 30 cm) o que utilicen canaletas con divisiones metálicas internas blindadas para evitar problemas de intermitencia de red por interferencia electromagnética.

💡 **Mantén un código de colores y peinado impecable en tus racks:** Implementa un estándar estricto de cableado estructurado: utiliza organizadores horizontales/verticales y asigna colores específicos (por ejemplo: azul para datos de usuarios, rojo para servidores y amarillo para telefonía) para identificar de inmediato cualquier anomalía.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará los planos o diagramas del cableado estructurado y las memorias técnicas de las pruebas de certificación de los nodos de red. Durante la auditoría física, inspeccionará las canalizaciones en áreas comunes para verificar que los cables no queden expuestos ni colgando, comprobará que los armarios de telecomunicaciones secundarios ubicados en los pasillos de las oficinas tengan candado o cerradura funcional, y seleccionará al azar un puerto de red desocupado en una sala de juntas pública para conectar un dispositivo de prueba y constatar si la organización bloquea eficazmente los accesos no autorizados a nivel de puerto físico.



Cláusula 7: Controles Físicos

Control 7.13 Mantenimiento de equipos

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

- **El Control:** El equipo debe mantenerse correctamente para garantizar su disponibilidad e integridad continuas.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en establecer una estrategia de mantenimiento sistemático sobre el hardware y los sistemas de soporte para prevenir fallos operativos, pérdida de datos o degradación del rendimiento. Los puntos clave resumidos son:
 - Programa de Mantenimiento Preventivo:** La organización debe contar con un calendario formalizado para realizar mantenimientos periódicos y preventivos de todos los equipos críticos (servidores, almacenamiento, plantas de energía, aires acondicionados), basándose en las especificaciones de los fabricantes.
 - Personal Autorizado:** Las tareas de mantenimiento técnico deben ser ejecutadas únicamente por personal calificado y debidamente autorizado. Cuando intervengan proveedores externos, sus actividades deben ser estrictamente supervisión y sus niveles de acceso lógico al sistema deben ser acotados y revocados al finalizar.
 - Control de Reparaciones Fuera de Sitio:** Si un equipo que contiene medios de almacenamiento debe salir de las instalaciones para reparación, los datos confidenciales deben ser cifrados o destruidos previamente.
 - Registro de Bitácoras:** Se debe documentar minuciosamente cada intervención realizada sobre los equipos, detallando la fecha, el tipo de mantenimiento (preventivo o correctivo), los fallos detectados, las piezas sustituidas y el nombre del técnico responsable.



Cláusula 7: Controles Físicos

Control 7.13 Mantenimiento de equipos

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

- **Otra Información:** La norma advierte que el mantenimiento deficiente no solo afecta la disponibilidad (caídas del sistema), sino que también puede comprometer la integridad de la información debido a corrupciones de hardware causadas por sobrecalentamiento, fallos de disco o fluctuaciones de energía. Además, destaca que los contratos de mantenimiento con terceros deben incluir cláusulas claras de confidencialidad (NDA) e indicar los tiempos de respuesta acordados (SLA) para reparaciones urgentes.

💡 **Exige el borrado seguro o extracción de discos antes de enviar a garantía:** Establece como política obligatoria que el equipo de soporte técnico extraiga físicamente el disco duro antes de entregar el equipo al proveedor, o bien, aplique un borrado seguro de bajo nivel si el hardware aún lo permite.

💡 **Administra los accesos remotos de los proveedores de soporte:** Asegúrate de que estas sesiones remotas utilicen contraseñas temporales de un solo uso (OTP), estén supervisadas visualmente por un ingeniero interno en tiempo real y que los accesos se desactiven inmediatamente después de que el proveedor termine su labor.

💡 **El Enfoque del Auditor (Lo que te van a revisar):**El auditor solicitará el Programa Anual de Mantenimiento Preventivo de los equipos de cómputo e infraestructura de soporte, así como el historial de las bitácoras o reportes de servicio correspondientes. Para verificar su cumplimiento operacional, seleccionará una muestra de activos críticos del inventario y pedirá los comprobantes de los mantenimientos ejecutados en las fechas programadas; asimismo, revisará los registros de salida de hardware que fue enviado a talleres externos para constatar que existió una orden formal de trabajo y evidencia del borrado o protección de los datos internos, validando finalmente las cláusulas de confidencialidad en los contratos vigentes de los proveedores encargados de dar soporte.



Cláusula 7: Controles Físicos

Control 7.14 Eliminación segura o reutilización de equipos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Seguridad física # Gestión de activos	# Protección

- **El Control:** Los elementos de equipo que contienen medios de almacenamiento deben verificarse para garantizar que cualquier dato sensible y software con licencia haya sido eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
- **Resumen de las Directrices de Implementación:** La guía de implementación busca evitar la fuga inadvertida de propiedad intelectual, datos personales o credenciales cuando los dispositivos tecnológicos cambian de dueño o son desechados como basura electrónica. Los puntos clave resumidos son:
 - Saneamiento de Medios (Sanitization):** Antes de vender, donar, devolver (si es arrendado) o desechar cualquier equipo con capacidad de almacenamiento, se debe aplicar un proceso de destrucción lógica o física de la información que impida su recuperación posterior mediante herramientas forenses.
 - Eliminación de Licencias y Configuración:** No basta con borrar los archivos del usuario; se debe remover por completo el sistema operativo corporativo, las configuraciones de red, las llaves criptográficas y el software con licencia de la empresa para evitar infracciones de propiedad intelectual o la exposición de la arquitectura de TI interna.
 - Evaluación del Destino:** El método de saneamiento debe depender de la criticidad del equipo. Si un disco duro contenía secretos comerciales de alto impacto, se debe priorizar la destrucción física destructiva (trituration) por encima del borrado lógico.
 - Identificación de Almacenamiento Oculto:** El control exige inspeccionar y purgar todo tipo de hardware que posea memoria interna, lo cual abarca no solo computadoras y servidores, sino también teléfonos inteligentes, ruteadores, conmutadores y equipos de impresión multifuncionales.



Cláusula 7: Controles Físicos

Control 7.14 Eliminación segura o reutilización de equipos

- **Otra Información:** La norma resalta la importancia de estándares internacionales de saneamiento de datos como la guía NIST SP 800-88 (Guidelines for Media Sanitization). Adicionalmente, advierte que los equipos dañados que no respondan a los comandos de software para un formateo seguro deben ser destruidos físicamente de inmediato a través de desmagnetización (degaussing) o pulverización mecánica para mitigar cualquier riesgo residual de recuperación de datos de los platos físicos o chips flash.

💡 **Establece la técnica de sobreescritura correcta antes de reutilizar:** Cuando vayas a reasignar la laptop de un empleado saliente a un nuevo colaborador de la empresa, el formateo tradicional de fábrica no es suficiente para garantizar la privacidad. Utiliza herramientas de borrado seguro certificadas que ejecuten al menos una pasada completa de sobreescritura con patrones aleatorios (método Purge o Clear) para asegurar que el nuevo usuario no pueda recuperar archivos privados del anterior inquilino.

💡 **Cuidado con los contratos de arrendamiento financiero (Leasing):** Diseña un protocolo estricto y documentado de purga de discos duros internos antes de que los equipos salgan de tus instalaciones de regreso al arrendador, evitando que tus bases de datos terminen en manos ajenas.

💡 **Mantén una bitácora de desecho amarrada al inventario:** Cada vez que un dispositivo se retire definitivamente de la operación, registra en tu sistema de gestión de activos (CMDB) la fecha de baja, el método de destrucción de datos aplicado (lógico o físico), el número de serie del componente y el nombre del ingeniero de soporte técnico que validó y firmó que el equipo quedó completamente limpio.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el procedimiento documentado para la baja, donación, venta o destrucción de equipos tecnológicos que contienen medios de almacenamiento. Para evaluar el control, seleccionará una muestra de equipos de cómputo, servidores o dispositivos de red que hayan sido dados de baja del inventario activo en el último ciclo; acto seguido, exigirá las evidencias técnicas y documentales (como los reportes generados por el software de borrado seguro o los certificados de destrucción física con los números de serie correspondientes) que certifiquen de manera inequívoca que los datos y el software con licencia fueron eliminados de forma irreversible antes de la salida definitiva.



Cláusula 8: Controles Tecnológicos

Control 8.1 Dispositivos de punto final de usuario

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

- **El Control:** La información almacenada en, procesada por o accesible a través de los dispositivos de punto final de usuario debe ser protegida.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar los dispositivos finales que utilizan los empleados (computadoras de escritorio, laptops, smartphones, tabletas) para interactuar con los recursos de la empresa. Los puntos clave resumidos son:
 - Gestión y Registro (Inventario):** Todos los dispositivos de punto final aprobados para el uso de la organización deben estar formalmente registrados en un inventario centralizado y administrados mediante herramientas de configuración.
 - Cifrado de Datos:** Para mitigar el riesgo de pérdida o robo del dispositivo, se debe exigir el cifrado total del disco duro y del almacenamiento local del equipo, protegiendo así la confidencialidad de los datos residuales.
 - Protección contra Malware y Actualizaciones:** Los endpoints deben contar con soluciones de software de protección (Antivirus/EDR) instaladas, configuradas para actualización automática de firmas y con bloqueo para que el usuario común no pueda desactivarlas. Asimismo, se debe forzar el parchado periódico del sistema operativo y aplicaciones.
 - Control de Acceso y Autenticación:** Se debe implementar la autenticación robusta mediante contraseñas seguras o biometría, acompañada de Autenticación de Múltiple Factor (MFA) para acceder a los servicios de la organización.
 - Uso Aceptable y Restricciones de Red:** Se deben deshabilitar o restringir puertos físicos innecesarios (como USB) y el uso de software no autorizado (privilegios de administrador local restringidos).



Cláusula 8: Controles Tecnológicos

Control 8.1 Dispositivos de punto final de usuario

- **Otra Información:** La norma resalta que, debido a la creciente adopción del trabajo remoto y políticas de Bring Your Own Device (BYOD), las organizaciones deben implementar soluciones de Gestión de Dispositivos Móviles (MDM) o Gestión de Movilidad Empresarial (EMM) para segregar la información corporativa de la personal y permitir el borrado remoto selectivo en caso de incidentes.

💡 **Elimina los privilegios de administrador local de inmediato:** Al requerir credenciales de TI para instalar cualquier programa, detienes de golpe más del 80% de las infecciones por malware o instalaciones de software pirata que abren brechas en la red.

💡 **Adopta una solución EDR en lugar de un antivirus tradicional:** Los antivirus basados únicamente en firmas ya no son suficientes para frenar las amenazas modernas como el ransomware de día cero. Invierte en soluciones EDR (Endpoint Detection and Response) que utilicen análisis de comportamiento e inteligencia artificial para detectar y aislar automáticamente un dispositivo final sospechoso antes de que infecte al resto de la empresa.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Seguridad para Dispositivos de Punto Final, las directrices de BYOD (si aplican) y el inventario técnico de hardware. Durante la evaluación, pedirá acceso a la consola centralizada de administración de endpoints (como Microsoft Intune, Active Directory o MDM) para extraer una muestra aleatoria de dispositivos activos; con ello verificará que los equipos tengan el cifrado de disco habilitado (BitLocker/FileVault), que el agente de Antivirus/EDR esté reportando en tiempo real con las firmas actualizadas, que no existan usuarios comunes listados en el grupo de administradores locales y que las directivas de bloqueo de pantalla e instalación de parches críticos se estén aplicando correctamente según la política establecida.



Cláusula 8: Controles Tecnológicos

Control 8.2 Derechos de acceso privilegiado

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Capacidad operativa Habilidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_ac- cess_management	# Proteccion

- **El Control:** La asignación y el uso de los derechos de acceso privilegiado deben ser restringidos y gestionados.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en proteger las cuentas con capacidades elevadas (como Administrador de Dominio, root, sa, administradores globales de la nube), ya que son el objetivo principal de los ciberatacantes. Los puntos clave resumidos son:
 - Identificación y Restricción:** Se deben identificar todas las cuentas y funciones que requieran privilegios elevados. Su asignación debe restringirse al mínimo número posible de usuarios basándose estrictamente en la necesidad del negocio y el principio de mínimo privilegio.
 - Proceso de Autorización Formal:** Ningún usuario debe obtener derechos privilegiados de forma automática. Se debe seguir un flujo de solicitud y aprobación formal, documentado y autorizado por los propietarios de los sistemas o el área de seguridad.
 - Segregación de Cuentas:** Los usuarios con funciones de administración no deben utilizar sus cuentas de privilegios elevados para tareas cotidianas (como revisar correo electrónico o navegar por internet).
 - Autenticación Robusta y Caducidad:** El uso de Autenticación de Múltiple Factor (MFA) es mandatorio para todas las cuentas privilegiadas. Además, estos derechos deben revisarse periódicamente y expirar o ser revocados inmediatamente si el colaborador cambia de puesto o deja la organización.



Cláusula 8: Controles Tecnológicos

Control 8.2 Derechos de acceso privilegiado

- **Otra Información:** La norma resalta la conveniencia de adoptar herramientas tecnológicas avanzadas como las soluciones de Gestión de Accesos Privilegiados (PAM - Privileged Access Management). Estas herramientas permiten implementar esquemas de acceso "Justo a Tiempo" (Just-In-Time o JIT), donde los privilegios elevados se otorgan de forma temporal (por ejemplo, por dos horas) para realizar una tarea específica y se revocan automáticamente al concluir, manteniendo además una grabación completa en video o texto de la sesión del administrador.

💡 **Separa las funciones de tus administradores desde hoy:** Es un riesgo crítico que tu Director de TI o Administrador de Redes use la misma cuenta con derechos de "Domain Admin" para responder correos de clientes o descargar archivos. Fuerza el uso de dos cuentas: una genérica para el día a día y una cuenta de administración dedicada protegida con un MFA extremadamente estricto que solo usará cuando deba configurar la infraestructura.

💡 **Adiós a las cuentas genéricas como "Administrator" o "Root":** El uso de credenciales compartidas destruye el principio de no repudio porque, si algo falla o se borra, es imposible saber quién fue. Deshabilita o renombra las cuentas de administrador genéricas del sistema operativo e implementa accesos privilegiados nominales (con nombre y apellido) o utiliza una bóveda de contraseñas que rote las claves automáticamente tras cada uso.

💡 **Implementa flujos de acceso "Justo a Tiempo" (JIT):** Nadie debería tener privilegios de administrador global activos las 24 horas del día de manera permanente. Utiliza herramientas que permitan "solicitar" el rol de administrador solo cuando vayan a ejecutar un mantenimiento programado; el sistema les otorgará el acceso de forma controlada por un tiempo limitado y, al vencer el plazo, volverán a ser usuarios estándar, reduciendo drásticamente la superficie de ataque.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Asignación de Accesos Privilegiados y el listado de usuarios que cuentan con perfiles de administrador en tus sistemas críticos, extraerá una muestra de estas cuentas privilegiadas y te pedirá demostrar en vivo que tienen habilitado el Múltiple Factor de Autenticación (MFA) de forma obligatoria; asimismo, solicitará los formatos de autorización firmados que justifican por qué se otorgaron dichos accesos.



Cláusula 8: Controles Tecnológicos

Control 8.3 Restricción de acceso a la información

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

- **El Control:** El acceso a la información y a las instalaciones de procesamiento de información debe restringirse de acuerdo con la política específica establecida sobre el control de acceso.
- **Resumen de las Directrices de Implementación:** La guía de implementación se centra en asegurar que los usuarios comunes (no privilegiados) solo puedan interactuar con la información que necesitan para realizar su trabajo diario, aplicando el principio de "necesidad de conocer" (need-to-know). Los puntos clave resumidos son:
 - Control de Acceso Lógico Basado en Roles (RBAC):** Se deben asignar los permisos a carpetas, aplicaciones, archivos y bases de datos agrupando a los usuarios en "roles" o "perfiles" (ej. Finanzas, Recursos Humanos, Operaciones), evitando asignar permisos individuales a nivel de usuario nominal para facilitar la gestión.
 - Mecanismos de Restricción Efectivos:** Los sistemas informáticos deben configurarse para ocultar o bloquear menús, transacciones, módulos o archivos a los cuales el usuario no tiene autorización explícita para entrar, leer, modificar o eliminar.
 - Control de Salida y Escritura:** No basta con restringir quién lee la información; se debe controlar quién puede copiarla, enviarla por correo, descargarla o imprimirla. Para datos altamente confidenciales, se deben implementar controles de solo lectura.
 - Revisión y Depuración Continua:** Las matrices de acceso y los permisos sobre carpetas compartidas o repositorios en la nube deben ser revisados de forma periódica por los dueños de la información para dar de baja accesos obsoletos.



Cláusula 8: Controles Tecnológicos

Control 8.3 Restricción de acceso a la información

- **Otra Información:** La norma resalta que se deben tomar en consideración los requisitos regulatorios de cumplimiento y protección de datos (como el resguardo de información financiera o datos personales de clientes). Asimismo, aconseja que el software de desarrollo propio o comercial cuente con capacidades nativas para auditar quién accedió a qué registros de información, garantizando la trazabilidad en caso de sospecha de fuga de datos.

💡 **Fuerza el principio de mínimo privilegio en tus carpetas compartidas:** El peor error en un servidor de archivos o almacenamiento en la nube (como OneDrive, Google Drive o Sharepoint) es dejar carpetas críticas con acceso para el grupo "Todos" o "Usuarios del Dominio". Configura tus sistemas partiendo de la premisa de "Denegar todo por defecto" y ve abriendo la llave de los accesos de manera quirúrgica y documentada.

💡 **Bloquea la fuga de datos con políticas de DLP:** Restringir el acceso dentro del sistema es solo la mitad del trabajo; la otra mitad es evitar que la información salga de ahí. Implementa soluciones de Prevención de Fuga de Datos (DLP) que bloqueen la capacidad de copiar texto confidencial, tomar capturas de pantalla o subir archivos clasificados a nubes públicas personales, manteniendo los datos protegidos dentro de las fronteras controladas de la empresa.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Control de Acceso y la Matriz de Roles y Permisos que detalla qué departamentos tienen derecho a ver qué información de la empresa. Para validar el control, seleccionará muestras de sistemas críticos (como el ERP, el CRM o el almacenamiento de archivos compartidos) y auditará de manera técnica los permisos asignados a carpetas de alta confidencialidad (como Nóminas, Fórmulas o Contratos); el auditor comprobará visualmente que usuarios de un departamento (por ejemplo, Marketing) no tengan privilegios de lectura o escritura en directorios restringidos de otra área (como Finanzas), y revisará que existan evidencias de las revisiones periódicas de accesos firmadas por los líderes de cada proceso.



Cláusula 8: Controles Tecnológicos

Control 8.4 Acceso al código fuente

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Identidad_y_acceso_ administración #Aplicación_seguridad # Secure_configura- ción	# Proteccion

- **El Control:** El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debe gestionarse y restringirse adecuadamente.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en proteger la propiedad intelectual más valiosa de las empresas tecnológicas o que desarrollan software: su código base. El objetivo es evitar alteraciones maliciosas (sabotaje o inserción de malware) y la fuga de secretos comerciales. Los puntos clave resumidos son:
 - Restricción Estricta de Accesos:** El acceso al código fuente y a los repositorios (como GitHub, GitLab o Bitbucket) debe limitarse únicamente al personal de desarrollo autorizado. Los permisos de "escritura" o modificación deben ser sumamente restringidos.
 - Control de Versiones y Trazabilidad:** Se deben utilizar sistemas de gestión de configuración de software (Sistemas de Control de Versiones - VCS) para registrar de manera auditable qué programador hizo qué cambios, cuándo y por qué (mediante mensajes de commit obligatorios).
 - Segregación de Entornos:** Los desarrolladores no deben tener acceso directo al código que ya está corriendo en producción desde sus entornos locales de desarrollo. La actualización del código en los servidores productivos debe hacerse mediante procesos automatizados.
 - Protección de Herramientas y Librerías:** El control exige también asegurar el acceso a los servidores de desarrollo, herramientas de compilación y el uso de bibliotecas de terceros, verificando que estas últimas no contengan vulnerabilidades conocidas.



Cláusula 8: Controles Tecnológicos

Control 8.4 Acceso al código fuente

- **Otra Información:** La norma resalta que si por razones de negocio se requiere dar acceso al código fuente a contratistas externos o proveedores de software, se deben aplicar medidas de seguridad adicionales, como el uso de entornos virtuales de desarrollo controlados que impidan la descarga o copia local del código (sandbox), además de estar respaldados por estrictas penalizaciones en los contratos de propiedad intelectual.

💡 **Fuerza la revisión por pares mediante "Pull Requests":** Nunca permitas que un desarrollador suba código directamente a la rama principal de producción (main o master) sin supervisión. Implementa una política técnica en tu repositorio que exija obligatoriamente que al menos otro programador o un líder técnico revise, comente y apruebe el código (Peer Review) antes de que pueda ser integrado.

💡 **Implementa MFA obligatorio en tus repositorios de código:** Activa de forma mandatoria la Autenticación de Múltiple Factor (MFA) para todos los usuarios en plataformas como GitHub o GitLab, y deshabilita el uso de contraseñas por defecto a favor de llaves SSH seguras.

💡 **Automatiza la detección de credenciales expuestas (Secrets Scanning):** Configura herramientas automatizadas en tus repositorios que escaneen el código en tiempo real y bloqueen cualquier intento de subir cambios que contengan credenciales expuestas a la vista.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Desarrollo Seguro y el listado de usuarios con acceso a las plataformas de control de versiones de la empresa. Durante la auditoría, pedirá una demostración técnica en vivo de la configuración de los repositorios críticos para verificar que las ramas principales estén protegidas contra modificaciones directas, comprobará las bitácoras de auditoría de la plataforma para constatar la trazabilidad de los cambios (commits), validará que los desarrolladores dados de baja recientemente hayan sido eliminados del sistema de control de versiones de forma inmediata, y revisará que existan evidencias de revisiones y aprobaciones previas al despliegue de código a producción.



Cláusula 8: Controles Tecnológicos

Control 8.5 Autenticación segura

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

- **El Control:** Se deben implementar tecnologías y procedimientos de autenticación segura basados en las restricciones de acceso a la información y en la política específica sobre el control de acceso.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en establecer los mecanismos técnicos para validar la identidad de un usuario, proceso o dispositivo que intenta conectarse a los sistemas de la organización, asegurando que nadie pueda suplantar una identidad legítima. Los puntos clave resumidos son:
 - Fortaleza de las Credenciales:** Se deben definir reglas estrictas para la creación de contraseñas complejas (longitud mínima, mezcla de caracteres) o, preferentemente, transicionar hacia métodos criptográficos avanzados y esquemas libres de contraseñas (passwordless).
 - Autenticación de Múltiple Factor (MFA):** Para accesos remotos, sistemas críticos, cuentas con privilegios elevados o datos confidenciales, el uso de MFA es mandatorio. Debe combinar al menos dos factores distintos: algo que sabes (contraseña/PIN), algo que tienes (token/celular) o algo que eres (biometría).
 - Gestión Segura de Contraseñas:** Si se usan contraseñas, los sistemas deben almacenarlas utilizando funciones de hash seguras con sal (salted hashing). Nunca deben transmitirse ni guardarse en texto plano.
 - Control de Intentos y Bloqueo:** Los sistemas deben limitar los intentos de inicio de sesión fallidos. Ante múltiples errores consecutivos, la cuenta debe bloquearse temporalmente o requerir un retraso progresivo para mitigar ataques de fuerza bruta o diccionario.
 - Retroalimentación Limitada:** Al fallar una autenticación, el sistema no debe dar pistas específicas (evitar mensajes como "La contraseña es incorrecta" o "El usuario no existe"). El mensaje debe ser genérico: "Usuario o contraseña incorrectos".



Cláusula 8: Controles Tecnológicos

Control 8.5 Autenticación segura

- **Otra Información:** La norma resalta que se deben evitar los identificadores de usuario (IDs) compartidos para no perder el principio de responsabilidad individual (no repudio). Asimismo, desaconseja el uso de sistemas de autenticación basados únicamente en SMS o llamadas telefónicas de voz para el MFA, ya que son vulnerables a ataques de intercambio de SIM (SIM swapping), sugiriendo en su lugar el uso de aplicaciones de autenticación dedicadas (como Google u Microsoft Authenticator) o llaves físicas de seguridad (FIDO2).

💡 **Haz del MFA la regla, no la excepción:** Implementa Autenticación de Múltiple Factor (MFA) de forma obligatoria para el 100% de los servicios de la empresa (correo corporativo, VPN, ERP, nubes) y configura políticas de acceso condicional que bloqueen inicios de sesión desde ubicaciones geográficas inusuales o IPs sospechosas.

💡 **Adopta una arquitectura moderna con Single Sign-On (SSO):** Centraliza la autenticación mediante un proveedor de identidad robusto con SSO; de esta manera, el usuario se autentica de forma ultra-segura una sola vez y accede a todas sus herramientas autorizadas.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Control de Acceso y los estándares técnicos de configuración de contraseñas y autenticación de la empresa. Para validar el control en la práctica, pedirá evidencias de configuración en vivo de los sistemas principales (como el Directorio Activo o la consola de administración de la nube); el auditor revisará que los parámetros de bloqueo por intentos fallidos estén activos, que las contraseñas exijan complejidad y longitud normadas, que no existan cuentas genéricas activas sin justificación y exigirá comprobar que las directivas de MFA estén configuradas como "Obligatorias" (Enforced) para todos los usuarios remotos y administradores del sistema.



Cláusula 8: Controles Tecnológicos

Control 8.6 Gestión de la capacidad

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Integridad # Disponibilidad	# Identificar # Proteger # Detectar	# Continuidad	# Gobernanza_y_ Ecosistema # Protección ción

- **El Control:** El uso de los recursos debe ser monitoreado y ajustado de acuerdo con los requisitos de capacidad actuales y esperados.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar la disponibilidad continua de los sistemas mediante una proactiva planeación y dimensionamiento de la infraestructura tecnológica, evitando caídas por saturación de recursos. Los puntos clave resumidos son:
 - Monitoreo Continuo de Recursos:** La organización debe supervisar métricas clave de rendimiento en tiempo real, tales como el uso de CPU, memoria RAM, espacio en disco duro, ancho de banda de red y capacidades de procesamiento de transacciones.
 - Proyecciones y Tendencias:** No basta con saber qué pasa hoy; se deben analizar los datos históricos de consumo para identificar tendencias de crecimiento a mediano y largo plazo, permitiendo a la empresa presupuestar y adquirir más capacidad antes de un problema.
 - Ajuste y Optimización:** Ante cuellos de botella detectados o previstos, se deben aplicar ajustes proactivos, como la actualización de hardware, la reasignación dinámica de recursos en entornos de nube, la depuración de datos obsoletos o la optimización del código de las aplicaciones.
 - Identificación de Puntos Críticos:** Se deben establecer umbrales mínimos y máximos de alerta (ej. notificar al equipo técnico cuando el almacenamiento en disco llegue al 80%).



Cláusula 8: Controles Tecnológicos

Control 8.6 Gestión de la capacidad

- **Otra Información:** La norma resalta que una mala gestión de la capacidad puede ser aprovechada por ciberatacantes para provocar una denegación de servicio (DoS) de forma más sencilla. Asimismo, en el entorno de computación en la nube, este control está estrechamente ligado a la gestión de costos, ya que una mala planeación puede derivar en un sobreaprovisionamiento innecesario o, por el contrario, en una degradación del servicio por falta de recursos.

💡 Establece alertas automáticas escalonadas en tus sistemas: Configura tu software de monitoreo (como Zabbix, Nagios o Datadog) para que envíe alertas preventivas basadas en umbrales inteligentes. Por ejemplo, una alerta de advertencia cuando el disco de la base de datos llegue al 80%, una alerta crítica al 90% y una automatización que expanda el volumen si llega al 95%, evitando que el sistema colapse por falta de espacio.

💡 **Planea la capacidad alineado al calendario del negocio:** La gestión de la capacidad no es solo un tema técnico de TI, sino operativo. Reúnete con las áreas de negocio para anticipar eventos de alta demanda comercial (como el Black Friday, cierres de año fiscal o campañas masivas de marketing) y aprovisiona los servidores con suficiente antelación para soportar la carga transaccional esperada.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el Plan de Gestión de la Capacidad, los reportes de rendimiento históricos y las evidencias de configuración de las herramientas de monitoreo de TI. Para evaluar el control, pedirá que se le muestren los tableros (dashboards) en tiempo real de los servidores más críticos de la organización, validará los umbrales de alerta configurados en el sistema y revisará los registros de incidentes pasados para comprobar cómo reaccionó la empresa ante eventos donde se superó la capacidad de los recursos, buscando constatar que existe un proceso formal de escalación, análisis de tendencias y remediación proactiva.



Cláusula 8: Controles Tecnológicos

Control 8.7 Protección contra malware

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Detectar	# Sistema_y_red_ seguridad # Information_protec- ción	# Proteccion # Defensa

- **El Control:** La protección contra el malware debe implementarse y respaldarse con la concientización adecuada del usuario.
- **Resumen de las Directrices de Implementación:** La guía de implementación aborda la necesidad de una estrategia de defensa en capas para detectar, prevenir y recuperarse de software malicioso (virus, ransomware, troyanos, spyware). Los puntos clave resumidos son:
 - Detección en Endpoints y Servidores:** Se deben instalar soluciones antimalware avanzadas en todos los dispositivos finales (laptops, desktops, smartphones) y servidores. Las firmas y los motores de detección deben actualizarse automáticamente de forma centralizada.
 - Seguridad en Canales de Entrada:** El malware suele ingresar por el correo electrónico o la navegación web. Es obligatorio implementar filtros de seguridad en las puertas de enlace (Gateways), analizando adjuntos en entornos seguros (sandboxing) y bloqueando el acceso a sitios web maliciosos conocidos.
 - Restricción de Privilegios y Software:** Para mitigar el impacto de una infección, se deben restringir los privilegios de administrador local a los usuarios y bloquear la ejecución de scripts o software que no esté explícitamente listado en una política de aplicaciones permitidas.
 - Concientización del Usuario:** La tecnología es inútil si el usuario ejecuta el archivo dañino. Se debe capacitar continuamente al personal para identificar correos sospechosos, enlaces de phishing y los peligros de conectar dispositivos USB desconocidos.
 - Planes de Contingencia y Aislamiento:** En caso de infección, se deben definir procedimientos rápidos para aislar los equipos comprometidos de la red interna, evitando el movimiento lateral del malware, y activar los mecanismos de restauración mediante respaldos limpios.



Cláusula 8: Controles Tecnológicos

Control 8.7 Protección contra malware

- **Otra Información:** La norma resalta que las firmas tradicionales de antivirus ya no bastan contra ataques dirigidos o malware polimórfico de día cero. Por ello, promueve el uso de tecnologías basadas en análisis de comportamiento e inteligencia artificial (como EDR/XDR). También advierte la importancia de escanear los archivos que los usuarios suben a las plataformas en la nube compartidas de la organización para evitar que actúen como focos de infección interna.

💡 **Migra del antivirus tradicional a una solución EDR/XDR centralizada:** Implementa una solución de Detección y Respuesta en Endpoints (EDR) que analice de manera proactiva el comportamiento de los procesos del sistema; si un programa desconocido intenta cifrar archivos masivamente, el EDR lo detendrá e aislará el equipo antes de que el ransomware se propague.

💡 **Blindar el correo electrónico con protección de adjuntos en la nube:** Activa soluciones avanzadas de seguridad de correo (como herramientas de análisis heurístico o sandboxing de archivos), las cuales abren y prueban de forma virtual los archivos adjuntos antes de que lleguen a la bandeja de entrada del usuario final.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Protección contra Malware y los estándares técnicos de configuración de las herramientas antimalware de la organización. Durante la revisión técnica, pedirá acceso a la consola centralizada de administración del Antivirus/EDR para evaluar una muestra de servidores y equipos finales; con esto comprobará que el 100% de los agentes asignados estén activos, con la protección en tiempo real encendida y reportando con las firmas o modelos de comportamiento al día, revisando asimismo las configuraciones de los filtros perimetrales de correo y navegación web.



Cláusula 8: Controles Tecnológicos

Control 8.8 Gestión de vulnerabilidades técnicas

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar # Proteger	# amenaza_y_ vulnerabilidad_ administración	# Gobernanza_y_Ecosistema # Protección #Defensa

- **El Control:** Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben tomar las medidas adecuadas para hacer frente al riesgo asociado.
- **Resumen de las Directrices de Implementación:** La guía de implementación detalla el ciclo de vida indispensable para descubrir y corregir las debilidades de seguridad en el software, firmware y hardware antes de que sean explotadas por atacantes. Los puntos clave resumidos son:
 - Obtención de Información:** La organización debe monitorear constantemente fuentes confiables de alertas de seguridad (como boletines de fabricantes, bases de datos como el NVD de NIST, CERTs nacionales y alertas CVE) para identificar fallos que afecten a su infraestructura tecnológica actual.
 - Evaluación de la Exposición (Análisis de Riesgo):** Una vez identificada una vulnerabilidad, se debe calcular el riesgo real para la empresa. Esto implica cruzar la criticidad del fallo (por ejemplo, su puntuación CVSS) con la importancia del activo afectado (si el servidor está expuesto a internet o si está aislado internamente).
 - Tratamiento y Remediación:** Se deben definir plazos específicos (SLAs) para mitigar los riesgos. Las acciones incluyen la aplicación de parches de seguridad, actualizaciones de software o parches virtuales. Si no hay parche disponible, se deben aplicar controles compensatorios (como reglas en el Firewall o aislamiento de red).
 - Roles y Responsabilidades:** Se debe delimitar claramente quién identifica la vulnerabilidad (ej. el equipo de ciberseguridad) y quién ejecuta la corrección (ej. los administradores de sistemas o bases de datos), manteniendo una separación de funciones adecuada.



Cláusula 8: Controles Tecnológicos

Control 8.8 Gestión de vulnerabilidades técnicas

- **Otra Información:** La norma advierte que el proceso de gestión de vulnerabilidades debe ser respaldado por un inventario de activos de información preciso y actualizado; de lo contrario, es imposible saber si una nueva alerta CVE afecta a la organización. Asimismo, resalta la importancia de realizar análisis periódicos de vulnerabilidades (Vulnerability Scans) y pruebas de penetración (Penetration Testing) para validar la efectividad de las correcciones aplicadas.

💡 **Estructura una matriz de tiempos de parchado basados en riesgo:** No intentes corregir todas las vulnerabilidades al mismo tiempo porque saturarás al equipo de TI. Define plazos de atención claros y obligatorios en tu política.

💡 **Prueba los parches en un entorno de desarrollo antes de ir a producción:** Mantenga siempre un entorno espejo (Staging/QA) donde se instalen los parches primero para validar que la aplicación del negocio siga funcionando correctamente bajo condiciones normales.

💡 **Implementa escaneos automatizados y continuos:** Utiliza herramientas de escaneo automatizado (como Nessus, Qualys o Greenbone) programadas de manera semanal para descubrir fallos de configuración o sistemas desactualizados en tu red interna y perimetral de forma proactiva.

💡 **El Enfoque del Auditor (Lo que te van a revisión):** El auditor solicitará el Procedimiento de Gestión de Vulnerabilidades Técnicas y el último Reporte de Análisis de Vulnerabilidades o Prueba de Penetración (Pentest) ejecutado por la organización. Para evaluar el control en la práctica, seleccionará una muestra de las vulnerabilidades críticas o altas detectadas en dicho reporte y exigirá las evidencias técnicas (como tickets de soporte, cambios autorizados en producción y capturas de pantalla de la versión de software actualizada) que demuestren que los fallos fueron corregidos o mitigados dentro de los plazos establecidos en tu propia política interna, verificando además la trazabilidad de los parches aplicados a los sistemas operativos principales.



Cláusula 8: Controles Tecnológicos

Control 8.9 Gestión de la configuración

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

- **El Control:** Las configuraciones, incluidas las configuraciones de seguridad, del hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
- **Resumen de las Directrices de Implementación:** La guía de implementación se centra en garantizar que los sistemas tecnológicos se desplieguen y mantengan bajo parámetros de configuración seguros y estandarizados durante todo su ciclo de vida, evitando el uso de configuraciones por defecto que suelen ser vulnerables. Los puntos clave resumidos son:
 - Establecimiento de Líneas Base (Baselines):** Se deben definir y documentar plantillas de configuración segura (hardening baselines) para cada tipo de activo tecnológico (sistemas operativos, servidores web, bases de datos, dispositivos de red y servicios en la nube).
 - Eliminación de Valores por Defecto:** Se deben cambiar o desactivar de inmediato las contraseñas predeterminadas de fábrica, puertos no utilizados, servicios innecesarios y cuentas de usuario de muestra antes de poner cualquier equipo en producción.
 - Registro Centralizado (CMDB):** Las configuraciones deben registrarse en una Base de Datos de Gestión de la Configuración (CMDB) o inventario técnico equivalente, manteniendo el rastreo de versiones, parches aplicados y dependencias entre sistemas.
 - Gestión y Control de Cambios:** Cualquier modificación a la configuración de un equipo debe seguir un flujo formal de control de cambios, evitando ajustes "al vuelo" no documentados.
 - Detección de la Deriva de Configuración (Configuration Drift):** Se debe implementar un monitoreo continuo para identificar automáticamente cuándo la configuración de un sistema en producción se ha desviado de la línea base aprobada.



Cláusula 8: Controles Tecnológicos

Control 8.9 Gestión de la configuración

- **Otra Información:** La norma resalta que, en entornos modernos y en la nube, la gestión de la configuración se beneficia ampliamente del enfoque de Infraestructura como Código (IaC). Utilizar plantillas automatizadas permite desplegar servidores o redes con la configuración de seguridad preaprobada de forma idéntica, minimizando el error humano. Asimismo, recomienda apoyarse en estándares reconocidos de la industria, como los CIS Benchmarks (Center for Internet Security) o las guías STIGs de DISA.

💡 **Adopta los guías de Hardening de CIS Benchmarks:** No reinventes la rueda intentando adivinar qué parámetros apagar en un servidor Windows o Linux. Descarga las guías gratuitas del Center for Internet Security (CIS); estas ofrecen plantillas paso a paso probadas a nivel mundial para asegurar prácticamente cualquier sistema operativo, base de datos o dispositivo de red.

💡 **Automatiza el cumplimiento con herramientas de gestión de estado:** Si un administrador ingresa a un servidor y cambia un parámetro por error o malicia, el sistema automatizado detectará la desviación y reescribirá la configuración para regresarla a su estado seguro aprobado de forma automática.

💡 **Aplica el principio de "Servicios Mínimos Necesarios":** Configura tus imágenes de servidores para que únicamente tengan instalados los componentes estrictamente necesarios para su función; si un servidor es solo una base de datos, no tiene por qué tener activos servicios de impresión, transferencia de archivos FTP o entornos gráficos pesados.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política y los Estándares Documentados de Configuración Segura (Hardening) para cada tipo de tecnología utilizada en la organización. Para validar su cumplimiento operativo, seleccionará una muestra aleatoria de activos en producción (servidores, switches de red, bases de datos o cuentas de nube) y ejecutará o pedirá que se ejecute una comparación técnica en vivo entre los parámetros reales del activo y la línea base aprobada; el auditor buscará evidenciar que no existan contraseñas por defecto,



Cláusula 8: Controles Tecnológicos

Control 8.10 Eliminación de información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	#Información_pro- tección # Legal_and_compli- ance	# Proteccion

- **El Control:** La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea requerida.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en el borrado oportuno y definitivo de los datos lógicos para reducir el riesgo de exposición innecesaria de información confidencial y cumplir con las normativas legales de retención de datos. Los puntos clave resumidos son:
 - Cumplimiento de Retención y Leyes:** La eliminación de la información debe estar alineada con los calendarios de retención de la empresa y con los marcos legales aplicables (como las leyes de protección de datos personales y derecho al olvido).
 - Borrado Seguro en Todos los Entornos:** La información debe ser eliminada de forma efectiva no solo de las bases de datos de producción, sino también de respaldos (backups), entornos de desarrollo/pruebas, registros del sistema (logs) y repositorios en la nube.
 - Uso de Métodos de Borrado Certificados:** Para evitar la recuperación no autorizada mediante técnicas forenses, se deben emplear mecanismos de purga lógica aprobados (sobreescritura de datos, borrado criptográfico o formateo seguro de bajo nivel).
 - Automatización y Trazabilidad:** Se deben implementar políticas automatizadas de ciclo de vida de datos para que el borrado ocurra sin intervención humana cuando expire el periodo de conservación, generando registros de auditoría que demuestren la eliminación.



Cláusula 8: Controles Tecnológicos

Control 8.10 Eliminación de información

- **Otra Información:** La norma resalta la efectividad del Borrado Criptográfico (Crypto-shredding), especialmente en entornos de nube pública. Este método consiste en destruir de forma irreversible las llaves criptográficas que protegen los datos almacenados; al desaparecer la llave, la información retenida

💡 **Aplica Crypto-shredding para tus datos en la nube:** En la nube no tienes acceso físico a los discos para triturarlos. Si vas a dar de baja un contenedor de almacenamiento (S3, Blob Storage) o una base de datos con información sensible, asegúrate de haber cifrado los datos previamente con tu propia llave (KMS) y elimina la llave. Sin la clave, los datos remanentes son solo basura incomprensible.

💡 **Establece reglas de ciclo de vida automatizadas (ILM):** Configura políticas de Information Lifecycle Management en tus plataformas (como Microsoft 365 o Google Workspace) para que los correos o archivos en papelera se borren definitivamente tras 30 días, y los registros temporales se purguen automáticamente al cumplir su plazo legal.

💡 **No olvides los entornos de desarrollo y respaldos:** Asegúrate de que tus procedimientos de borrado contemplen la purga o anonimización periódica de estos ambientes secundarios.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Retención y Eliminación de Información de la organización. Para comprobar la efectividad del control, seleccionará una muestra de registros de datos que hayan cumplido su tiempo de vida útil (o solicitudes formales de eliminación de datos personales) y pedirá evidencias técnicas (como logs de ejecuciones de scripts de borrado, bitácoras de auditoría de la base de datos o destrucción de llaves criptográficas) que demuestren que los datos fueron borrados de forma irreversible en el sistema principal, verificando además cómo la empresa gestiona la eliminación de esa información dentro de sus esquemas de respaldos históricos.



Cláusula 8: Controles Tecnológicos

Control 8.11 Enmascaramiento de datos

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

- **El Control:** El enmascaramiento de datos debe utilizarse de acuerdo con la política específica sobre el control de acceso de la organización y otras políticas específicas relacionadas, así como con los requisitos del negocio, teniendo en cuenta la legislación aplicable.
- **Resumen de las Directrices de Implementation:** La guía de implementación se enfoca en proteger la información confidencial o sensible (como Datos de Identificación Personal - PII, números de tarjetas de crédito o información financiera) mediante técnicas que ocultan o reemplazan los datos reales para que no estén expuestos innecesariamente a usuarios o sistemas que no requieren verlos. Los puntos clave resumidos son:
 - Protección según Necesidad:** La información debe ocultarse en pantallas, reportes, entornos de prueba y desarrollo de forma que solo las personas con la debida autorización puedan visualizar los datos completos.
 - Técnicas Comunes de Enmascaramiento:**
 - Anonimización:** Modificación de datos de forma irreversible para que no puedan reidentificarse.
 - Seudonimización:** Reemplazo de datos reales por identificadores ficticios (se puede revertir mediante una clave o tabla separada guardada de forma segura).
 - Enmascaramiento Dinámico:** Ocultamiento en tiempo real sobre la pantalla del usuario (ej. mostrar solo los últimos 4 dígitos de una tarjeta).
 - Tokenización:** Reemplazo de datos sensibles por valores equivalentes no sensibles llamados "tokens".
 - Uso en Entornos No Productivos:** Se prohíbe el uso de bases de datos de producción con datos reales en entornos de desarrollo, pruebas o capacitación sin haber aplicado previamente un proceso de enmascaramiento estático e irreversible.
 - Cumplimiento Legal:** El uso de estas técnicas debe alinearse con marcos regulatorios como el GDPR, PCI-DSS o leyes locales de protección de datos personales.



Cláusula 8: Controles Tecnológicos

Control 8.11 Enmascaramiento de datos

- **Otra Información:** La norma resalta la diferencia entre el cifrado y el enmascaramiento: el cifrado protege los datos en tránsito o en reposo impidiendo el acceso no autorizado mediante claves criptográficas; el enmascaramiento, en cambio, permite que una aplicación o persona siga interactuando con la estructura del dato (por ejemplo, para pruebas de software) sin revelar el contenido sensible real.

💡 **Ofusca los datos antes de copiarlos al entorno de desarrollo:** Utiliza herramientas automatizadas de Data Masking estático que alteren los nombres, correos y saldos de forma realista pero falsa antes de restaurar el respaldo en QA o Staging.

💡 **Proteja los logs y registros del sistema:** Configura filtros en tu código para que datos como contraseñas, tokens de autenticación o números de tarjetas se enmascaren automáticamente antes de registrarse en herramientas como Splunk o ELK.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Enmascaramiento y Anonimización de Datos de la organización. Para comprobar el control, realizará una revisión doble: en primer lugar, inspeccionará las pantallas de las aplicaciones principales (como el CRM o ERP) con usuarios de diferentes roles para verificar que los datos sensibles aparezcan ocultos dinámicamente según el nivel de permisos; en segundo lugar, examinará los entornos de desarrollo, pruebas y capacitación para comprobar que las bases de datos utilizadas no contengan información personal o financiera real de clientes y empleados, pidiendo evidencia de los scripts o herramientas automatizadas empleadas para ofuscar los datos antes de su transferencia desde producción.



Cláusula 8: Controles Tecnológicos

Control 8.12 Prevención de fuga de datos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad	# Proteger #Detectar	#Información_pro- tección	# Proteccion # Defensa

El Control: Se deben aplicar medidas de prevención de fuga de datos a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

- **Resumen de las Directrices de Implementación:** La guía de implementación se centra en evitar la extracción, filtración o exfiltración no autorizada de datos confidenciales por parte de usuarios internos (de forma accidental o maliciosa) o atacantes externos. Los puntos clave resumidos son:
 - Identificación y Clasificación de Datos:** Antes de prevenir la fuga, la organización debe saber qué datos son sensibles (PII, secretos comerciales, finanzas) y dónde residen (en reposo, en tránsito o en uso).
 - Monitoreo y Detección en Canales de Salida:** Se deben supervisar los canales por los que la información puede salir de la organización, tales como:
 - Correo electrónico (adjuntos y cuerpo del mensaje).
 - Servicios de almacenamiento en la nube pública (OneDrive, Google Drive, Dropbox).
 - Dispositivos de almacenamiento extraíbles (memorias USB, discos externos).
 - Portapapeles, capturas de pantalla y servicios de mensajería instantánea.
 - Tráfico web en general (subida de archivos por HTTPS).
 - Acciones Automatizadas de Bloqueo: Las herramientas de Prevención de Pérdida de Datos (DLP - Data Loss Prevention) deben configurarse para alertar, restringir o bloquear automáticamente la transmisión de datos cuando detecten un patrón o etiqueta de clasificación confidencial.
 - Control de Canales Remotos:** En esquemas de teletrabajo o dispositivos móviles, se debe impedir la copia de datos desde el entorno corporativo hacia escritorios o almacenamiento locales no gestionados.



Cláusula 8: Controles Tecnológicos

Control 8.12 Prevención de fuga de datos

- **Otra Información:** La norma resalta que los controles de DLP no solo deben ser tecnológicos, sino que requieren estar respaldados por el cumplimiento legal y la privacidad de los empleados. La supervisión del tráfico de red y correos debe realizarse dentro del marco de la legislación laboral vigente para evitar vulnerar los derechos de los trabajadores.

💡 **Comienza con DLP en modo "Solo Auditoría" (Audit Mode):** Un error grave al implementar herramientas de DLP es activar el modo de bloqueo total desde el primer día. Esto puede paralizar los procesos del negocio por falsos positivos. Mantén las reglas en modo supervisión durante un par de meses para entender el flujo real de datos de la empresa, ajustar las excepciones y recién ahí activar los bloqueos.

💡 **Combina DLP con etiquetas de clasificación (MIP/Purview):** La tecnología de DLP funciona mucho mejor cuando los archivos ya nacen "etiquetados". Utiliza soluciones de clasificación de información (como Microsoft Purview) para que, cuando un usuario cree un documento "Confidencial", el archivo lleve un sello o metadato interno que la herramienta de DLP reconozca y bloquee al instante si intenta salir por correo externo.

💡 **Bloquea los puertos USB mediante políticas centrales:** Si la función del empleado no requiere el uso de unidades externas, deshabilita la lectura/escritura en puertos USB mediante directivas de grupo (GPO) o herramientas de Endpoint Management.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Prevención de Fuga de Datos y la evidencia de la solución tecnológica implementada (DLP en Endpoint, Red o Nube). Durante la evaluación técnica, pedirá ingresar a la consola de administración del DLP para revisar las reglas activas de inspección en los canales principales (correo, web y USB); posteriormente, exigirá mostrar el historial de alertas o eventos de intento de exfiltración detectados, verificando la matriz de escalamiento e investigación de los incidentes generados por la herramienta para confirmar que la organización gestiona proactivamente los intentos de salida de información sensible.



Cláusula 8: Controles Tecnológicos

Control 8.13 Copia de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Correctivo	# Integridad # Disponibilidad	# recuperar	# Continuidad	# Proteccion

- **El Control:** Las copias de seguridad de la información, el software y los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política específica acordada sobre copias de seguridad.
- **Resumen de las Directrices de Implementación:** La guía de implementación busca garantizar la disponibilidad e integridad de los datos y sistemas para permitir una recuperación rápida y confiable ante incidentes como desastres naturales, fallos de hardware, borrados accidentales o ataques de ciberseguridad (como el ransomware). Los puntos clave resumidos son:
 - Definición de Métricas Operativas:** La estrategia de respaldo debe basarse en el RPO (Recovery Point Objective / Objetivo de Punto de Recuperación) para determinar la frecuencia de los respaldos, y en el RTO (Recovery Time Objective / Objetivo de Tiempo de Recuperación) para determinar la velocidad requerida en la restauración.
 - Alcance Completo:** No solo se deben respaldar las bases de datos o los archivos de los usuarios; la estrategia debe incluir imágenes del sistema operativo, configuraciones de red, código fuente, licencias y componentes clave de infraestructura.
 - Almacenamiento Seguro y Separación Geográfica:** Las copias de seguridad deben guardarse en una ubicación física o lógica independiente del sitio principal (por ejemplo, en un segundo centro de datos o en un contenedor de nube separado).
 - Protección y Cifrado de Respaldos:** Los respaldos deben protegerse con controles de acceso estrictos y cifrarse tanto en tránsito como en reposo para evitar que la información caiga en manos no autorizadas.
 - Pruebas Periódicas de Restauración:** Tener un respaldo no garantiza que funcione. Es obligatorio realizar simulacros regulares de restauración de datos para comprobar que los archivos no estén corruptos y que el proceso se complete dentro de los tiempos exigidos por el negocio.



Cláusula 8: Controles Tecnológicos

Control 8.13 Copia de seguridad de la información

- **Otra Información:** La norma resalta la importancia de la arquitectura Inmutable y Aislada (Air-Gapped) frente a la amenaza moderna del ransomware. Muchos malwares avanzados buscan deliberadamente los servidores de respaldo dentro de la red interna para cifrarlos o borrarlos antes de ejecutar el ataque principal. Mantener copias fuera de línea (offline) o con políticas de retención inalterables (WORM - Write Once, Read Many) neutraliza esta técnica de ataque.

💡 **Aplica la regla de oro 3-2-1-1-0 para tus respaldos:**

Guárdalas en 2 tipos de medios distintos y mantén 1 copia fuera de la oficina (off-site).

Asegúrate de que 1 copia sea completamente inmutable o esté aislada de la red (air-gapped).

💡 **Monitorea los tiempos de RPO/RTO reales, no los teóricos:** Realiza pruebas de restauración completas en un ambiente de pruebas y mide el tiempo real que toma desde que se descarga la copia hasta que la aplicación vuelve a estar arriba. Esos datos reales son los que presentarás al comité de crisis.

💡 **Aísla los permisos del repositorio de copias de seguridad:** Las credenciales que administran tus servidores en producción (como el Administrador del Dominio) no deben tener acceso con permisos de escritura o borrado al repositorio de respaldos. Si la red corporativa es comprometida, el atacante no podrá destruir los respaldos porque no tendrá las claves de esa consola independiente.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Copias de Seguridad, el esquema de retención y la matriz de RPO/RTO de la organización. Para validar el cumplimiento, revisará los registros diarios/semanales de ejecución exitosa de respaldos; asimismo, pedirá los informes firmados de los simulacros de restauración periódicos realizados en el último año y, de ser posible, solicitará una restauración en vivo de un archivo o base de datos aleatoria en un entorno de pruebas durante la misma auditoría para verificar la integridad de las copias y la eficacia del procedimiento.



Cláusula 8: Controles Tecnológicos

Control 8.14 Redundancia de las instalaciones de procesamiento de información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Disponibilidad	# Proteger	# Continuidad # Gestión de activos	# Protección # Resiliencia

- **El Control:** Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en diseñar e implementar arquitecturas tecnológicas con tolerancia a fallos, de modo que si un componente clave o un sitio completo falla, la operación del negocio no se interrumpa o la degradación del servicio sea mínima. Los puntos clave resumidos son:
 - Análisis de Requisitos de Disponibilidad:** La redundancia debe definirse en función de los requisitos de negocio, identificando los componentes críticos (puntos únicos de fallo / Single Points of Failure - SPOF) mediante análisis de impacto al negocio (BIA).
 - Redundancia de Hardware y Componentes:** Implementar componentes duplicados o múltiples dentro de la misma infraestructura, como fuentes de alimentación dobles, arreglos de discos (RAID), interfaces de red agregadas y clústeres de servidores (balanceo de carga).
 - Redundancia de Redes y Conectividad:** Contar con enlaces de comunicaciones y proveedores de internet (ISP) redundantes con rutas físicas diversas.
 - Redundancia de Sitios (Disaster Recovery Site):** Para servicios de ultra alta disponibilidad, se deben mantener centros de datos secundarios o arquitecturas multi-región/multi-zona en la nube con replicación de datos en tiempo real (activo-activo) o diferida (activo-pasivo).
 - Pruebas de Conmutación por Error (Failover):** Los mecanismos de redundancia y conmutación automática o manual deben probarse periódicamente para verificar que funcionan correctamente ante un fallo real sin corromper la información.



Cláusula 8: Controles Tecnológicos

Control 8.14 Redundancia de las instalaciones de procesamiento de información

- **Otra Información:** La norma resalta que la redundancia introduce una mayor complejidad arquitectónica y, en ocasiones, nuevos riesgos de seguridad o costos elevados de licenciamiento e infraestructura. Por ejemplo, en esquemas de replicación automática, si los datos del sitio principal se corrompen o se cifran por un ataque de ransomware, esa corrupción se replicará instantáneamente al sitio redundante. Por ello, la redundancia no sustituye a las copias de seguridad (8.13), sino que la complementa.

💡 **Elimina los Puntos Únicos de Fallo (SPOF) ocultos:** Revisa tu arquitectura de punta a punta. Tener dos servidores web no sirve de nada si ambos dependen de una sola base de datos o si pasan por un único switch de red. Asegúrate de duplicar cada eslabón de la cadena crítica (red, almacenamiento, cómputo y energía).

💡 **Aprovecha las zonas de disponibilidad de la nube (Multi-AZ):** Las plataformas en la nube facilitan la configuración de balanceadores de carga y replicación de bases de datos de forma casi nativa y a una fracción del costo de construir un segundo centro de datos físico.

💡 **Efectúa simulacros de conmutación real (Failover Tests):** Programa al menos una o dos veces al año un ejercicio de simulación donde desconectes intencionalmente el servidor o enlace primario para verificar que el tráfico conmute automáticamente al secundario dentro del tiempo esperado y sin perder sesiones de usuarios.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la arquitectura de red e infraestructura detallada, así como la matriz de Análisis de Impacto al Negocio (BIA) para comprobar qué niveles de disponibilidad exige la organización. Para evaluar la efectividad de este control, inspeccionará visual o lógicamente la configuración de clústeres, balanceadores de carga, arreglos de discos y redundancia de proveedores; posteriormente, pedirá los registros o minutas de las pruebas de conmutación (failover) más recientes para verificar que el mecanismo de conmutación automática o manual fue validado en la práctica y respondió dentro de los parámetros de disponibilidad pactados.



Cláusula 8: Controles Tecnológicos

Control 8.15 Registro

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

- **El Control:** Los registros que graban actividades, excepciones, fallos y otros eventos relevantes deben generarse, almacenarse, protegerse y analizarse.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en establecer la trazabilidad técnica necesaria para auditar el comportamiento de los sistemas, detectar anomalías de seguridad en tiempo real y permitir investigaciones forenses ante cualquier incidente. Los puntos clave resumidos son:
 - Eventos a Registrar:** Se deben capturar eventos relevantes como accesos de usuarios (exitosos y fallidos), uso de privilegios de administrador, cambios de configuración, excepciones o errores del sistema, modificaciones a datos críticos y activación de alertas de seguridad.
 - Información Mínima del Registro:** Cada entrada de log debe incluir, al menos: ID de usuario o dispositivo, fecha y hora exacta, tipo de evento, dirección IP/ubicación lógica y el resultado de la acción (éxito o fallo).
 - Protección de Bitácoras:** Los archivos de registro deben protegerse contra manipulación, borrado, alteración o lectura no autorizada, limitando los permisos de modificación incluso para los propios administradores del sistema.
 - Monitoreo y Análisis Centralizado:** Los logs no deben quedarse olvidados en los servidores locales. Se deben centralizar mediante herramientas automatizadas (como sistemas SIEM) para analizar eventos en tiempo real y correlacionar actividades sospechosas.
 - Tiempo de Retención:** Se deben definir plazos de conservación de bitácoras según las políticas internas, normativas legales y requisitos de auditoría de la industria.



Cláusula 8: Controles Tecnológicos

Control 8.15 Registro

- **Otra Información:** La norma advierte que el registro masivo e indiscriminado de eventos puede generar volúmenes desproporcionados de almacenamiento e impactar el rendimiento de los equipos (log flooding). Por ello, es vital aplicar un enfoque basado en riesgos para seleccionar qué eventos registrar. Asimismo, resalta que los logs no deben contener información confidencial expuesta en texto plano (como contraseñas, datos personales o números de tarjeta de crédito).

💡 **Centraliza tus registros en un SIEM o repositorio WORM:** Si un ciberatacante logra comprometer un servidor, lo primero que intentará hacer es borrar los logs locales para eliminar sus huellas. Configura el envío de registros en tiempo real hacia una plataforma centralizada (como SIEM o un almacenamiento tipo Write Once, Read Many); de esta forma, aunque el servidor sea destruido, la evidencia quedará resguardada fuera de su alcance.

💡 **Ofusca los datos sensibles antes de escribir la bitácora:** Si un atacante o usuario no autorizado obtiene acceso a los registros del sistema, no debería encontrar información confidencial al descubierto.

💡 **Define alertas automáticas basadas en comportamiento:** Crea reglas de correlación automatizadas que generen alertas inmediatas al equipo de ciberseguridad ante patrones sospechosos (por ejemplo: múltiples intentos fallidos de inicio de sesión seguidos de un acceso exitoso fuera del horario laboral habitual).

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Generación y Retención de Registros. Durante la revisión práctica, el auditor pedirá acceso a la consola de administración centralizada de logs y verificará que los eventos críticos (accesos a servidores, uso de privilegios de administrador, modificaciones en directorios) se estén registrando de forma activa; comprobará que los registros contengan la información mínima requerida (marcas de tiempo, ID de usuario, IP), validará que los permisos de los archivos de bitácora impidan su modificación o borrado por parte de los administradores locales y revisará evidencias de las alertas automáticas o revisiones periódicas generadas a partir del análisis de dichos eventos.



Cláusula 8: Controles Tecnológicos

Control 8.16 Actividades de seguimiento

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

- **El Control:** Las redes, sistemas y aplicaciones deben ser monitoreados para detectar comportamientos anómalos y se deben tomar las acciones adecuadas para evaluar posibles incidentes de seguridad de la información.
- **Resumen de las Directrices de Implementación:** Mientras que el control anterior (8.15 Logging) se encarga de la recolección y almacenamiento de las bitácoras de eventos, el control 8.16 aborda la supervisión activa y proactiva de esos datos. Su objetivo es detectar en tiempo real o casi real cualquier desviación del comportamiento normal que pueda indicar un ataque o una brecha de seguridad. Los puntos clave resumidos son:
 - Establecimiento de Líneas Base de Comportamiento:** Para poder identificar un comportamiento anómalo, la organización debe definir primero lo que se considera "funcionamiento normal" del tráfico de red, uso de recursos y actividades de usuario.
 - Sistemas de Monitoreo Continuo:** Implementar herramientas automatizadas de monitoreo de seguridad, tales como:
 - Sistemas de Detección/Prevención de Intrusos (IDS/IPS).
 - Monitoreo de Seguridad de Red (NSM).
 - Soluciones de Gestión de Eventos e Información de Seguridad (SIEM) o Detección y Respuesta Extendida (XDR).
 - Supervisión de Múltiples Capas:** El monitoreo debe cubrir de forma holística la red perimetral e interna, los servidores, las aplicaciones corporativas, los dispositivos de punto final (endpoints) y los servicios en la nube.
 - Respuesta e Investigación:** Al detectarse una anomalía o activarse una alerta de seguridad, se deben ejecutar flujos de trabajo claros para validar si se trata de un falso positivo o un incidente real, escalándolo de inmediato al equipo de respuesta a incidentes.



Cláusula 8: Controles Tecnológicos

Control 8.16 Actividades de seguimiento

- **Otra Información:** La norma destaca la adopción de tecnologías avanzadas como el Análisis de Comportamiento de Usuarios y Entidades (UEBA) y el uso de Inteligencia Artificial / Aprendizaje Automático (Machine Learning). Estas herramientas permiten identificar patrones sutiles que las reglas tradicionales basadas en firmas no detectan, como un empleado accediendo a volúmenes atípicos de datos a horas no habituales o conexiones desde ubicaciones geográficas imposibles.

💡 **Ajusta las alertas para evitar la "fatiga de alertas":** Un error muy común en los equipos de operaciones es configurar reglas de monitoreo demasiado sensibles. Recibir cientos de alertas diarias genera cansancio en el personal y provoca que los analistas ignoren eventos que sí representan una amenaza real. Calibra continuamente las reglas y enfócate en alertas de alto impacto y baja tasa de falsos positivos.

💡 **Monitorea el tráfico de red de salida (Egress Traffic):** Gran parte de las empresas concentran todo su monitoreo en lo que entra a la red. Sin embargo, cuando un atacante compromete un sistema, la primera señal evidente es la comunicación de salida hacia servidores externos de Comando y Control (C2) o la exfiltración masiva de datos. Supervisar el tráfico saliente es crucial para detectar intrusiones tempranas.

💡 **Define métricas e indicadores de rendimiento (KPIs) para el monitoreo:** Mide el desempeño de tu monitoreo con indicadores como el Tiempo Medio de Detección (MTTD - Mean Time to Detect) y el Tiempo Medio de Respuesta (MTTR - Mean Time to Respond).

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Procedimiento de Monitoreo de Seguridad y Operaciones de TI. Durante la auditoría, pedirá una demostración en vivo de las herramientas de supervisión (como el SIEM, XDR o la consola del SOC); verificará las reglas de detección de anomalías activas, la disponibilidad de tableros de monitoreo en tiempo real y exigirá una muestra de alertas de seguridad generadas en los últimos meses para comprobar que existió un análisis formal de cada evento, constatando la trazabilidad desde la generación del ticket de incidente hasta su resolución y cierre.



Cláusula 8: Controles Tecnológicos

Control 8.16 Actividades de seguimiento

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

- **El Control:** Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar que todos los componentes de la infraestructura tecnológica compartan exactamente la misma hora. Una desalineación temporal, aunque sea de pocos segundos o minutos, invalida la trazabilidad de los eventos y dificulta el análisis forense durante la investigación de un incidente. Los puntos clave resumidos son:
 - Fuente de Tiempo Autorizada:** La organización debe definir y utilizar fuentes de tiempo oficiales y altamente precisas, como servidores de tiempo basados en NTP (Network Time Protocol) vinculados al Tiempo Universal Coordinado (UTC) o sistemas de posicionamiento global (GPS/GNSS).
 - Servidores de Tiempo Internos (Estratos):** En lugar de que cada equipo de la empresa se conecte de forma independiente a servidores de tiempo externos en internet, se debe implementar una jerarquía interna (un servidor NTP interno principal que se sincronice con la fuente externa aprobada y distribuya la hora al resto de la red).
 - Sincronización Multicapa:** Se deben sincronizar los relojes de todos los dispositivos de la infraestructura.
 - Alertas por Desviación Temporal (Clock Drift):** Se debe implementar un monitoreo para detectar desfases temporales o desincronizaciones entre sistemas y generar alertas proactivas antes de que afecten la operación.



Cláusula 8: Controles Tecnológicos

Control 8.16 Actividades de seguimiento

- **Otra Información:** La norma resalta que la precisión de la hora es esencial para el correcto funcionamiento de los mecanismos de autenticación y cifrado modernos (como Kerberos, tokens de acceso temporal OTP o certificados digitales), los cuales rechazarán conexiones si detectan un desfase de tiempo (skew) entre el cliente y el servidor. Asimismo, la sincronización exacta es un requisito legal y regulatorio indispensable en industrias como la bancaria, de telecomunicaciones y mercados de valores para garantizar la validez jurídica de las transacciones financieras y las bitácoras presentadas ante tribunales.

💡 **Establece una jerarquía NTP interna y bloquea la salida directa a internet:** Configura dos o tres servidores NTP internos que actúen como fuente primaria para tu organización, y bloquea en el firewall cualquier tráfico NTP (Puerto UDP 123) saliente desde los demás equipos internos. Esto reduce el consumo de ancho de banda y evita posibles ataques de amplificación NTP.

💡 **Estandariza todos los logs en UTC:** Un dolor de cabeza muy común durante la investigación de una brecha de seguridad es reconstruir la línea de tiempo cuando unos servidores registran eventos en hora local (ej. GMT-6) y otros en hora UTC (GMT+0). Configura todos los servidores y dispositivos de red para que guarden sus bitácoras de eventos estrictamente en formato UTC.

💡 **Monitorea los fallos de sincronización con alertas automatizadas:** Configura tu herramienta de monitoreo de TI para que supervise la diferencia de tiempo entre los endpoints y el servidor NTP central; si un servidor supera un desfase de más de 5 segundos, genera un ticket de atención técnica.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Sincronización del Reloj de la organización y el diagrama de la arquitectura del protocolo de tiempo (NTP). Para validar el cumplimiento, seleccionará una muestra diversa de activos tecnológicos (servidores Windows/Linux, firewalls perimetrales, bases de datos y consolas de virtualización) y pedirá ejecutar comandos en vivo en la terminal el auditor verificará que todos los sistemas utilicen la fuente de tiempo interna autorizada, que las zonas horarias estén estandarizadas correctamente y que el desfase temporal con respecto a la fuente UTC sea imperceptible o nulo.



Cláusula 8: Controles Tecnológicos

Control 8.17 Sincronización del reloj

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Detective	# Integridad	# Proteger #Detectar	# Information_securi- ty_event_management	# Proteccion # Defensa

- **El Control:** Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar que todos los componentes de la infraestructura tecnológica compartan exactamente la misma hora de referencia. La desalineación temporal invalida la trazabilidad de los eventos y dificulta el análisis forense durante la investigación de un incidente. Los puntos clave resumidos son:
 - Fuente de Tiempo Aprobada:** La organización debe definir y utilizar fuentes de tiempo oficiales y precisas, basadas en NTP (Network Time Protocol) vinculadas al Tiempo Universal Coordinado (UTC) o sistemas de posicionamiento satelital (GPS/GNSS).
 - Jerarquía Interna de Sincronización:** En lugar de permitir que cada dispositivo consulte servidores de tiempo externos por separado, se debe estructurar una jerarquía interna (servidores NTP primarios internos que consulten la fuente aprobada y redistribuyan la hora a la red local).
 - Cobertura Integral:** La sincronización debe aplicar a todos los activos de procesamiento: servidores de aplicaciones, bases de datos, dispositivos de red (switches, routers, firewalls), hipervisores, estaciones de trabajo y sistemas de control de acceso físico/videovigilancia.
 - Monitoreo de Desviación (Clock Drift):** Se deben supervisar los desfases de reloj entre los sistemas para detectar anomalías o pérdidas de sincronización de manera oportuna.



Cláusula 8: Controles Tecnológicos

Control 8.17 Sincronización del reloj

- **Otra Información:** La norma destaca que la precisión temporal es un requisito técnico indispensable para protocolos de autenticación basados en tickets o marcas de tiempo (como Kerberos), certificados digitales y autenticación de un solo uso (TOTP), los cuales rechazan intentos de acceso si detectan desfases temporales (clock skew). Asimismo, la sincronización es crítica para cumplir con requerimientos legales, regulatorios y probatorios en auditorías o litigios donde las marcas de tiempo de las bitácoras (timestamps) constituyen evidencia jurídica.



Centraliza la salida NTP y cierra el puerto en el perímetro: Configura dos o tres servidores NTP internos que actúen como fuente autorizada para toda la empresa y bloquea en el firewall el tráfico saliente por el puerto UDP 123 desde el resto de los dispositivos. Esto evita consumo innecesario de ancho de banda y mitiga riesgos de envenenamiento o ataques de amplificación NTP.



Estandariza los registros de eventos en formato UTC: Para evitar confusiones durante análisis forenses entre sistemas ubicados en distintas zonas horarias o con cambios por horario de verano, configura todos los servidores, bases de datos y herramientas de monitoreo para que almacenen sus marcas de tiempo estrictamente en formato UTC.



Configura alertas automáticas por desfase temporal: Las fallas de sincronización suelen ocurrir de forma silenciosa por problemas de conectividad o fallas en la batería de la placa base. Establece alertas en la herramienta de monitoreo cuando la diferencia temporal de un equipo supere los 3 a 5 segundos con respecto al servidor de referencia.



El Enfoque del Auditor (Lo que te van a revisar): El auditor solicitará la Política de Sincronización de Tiempo y el diagrama de la arquitectura del protocolo NTP. Para verificar el control en la práctica, seleccionará una muestra representativa de activos (servidores Windows/Linux, firewalls perimetrales, bases de datos y controladores de dominio) y solicitará ejecutar comandos de verificación en tiempo real (como `w32tm /query /status` en Windows o `chronyc tracking / ntpstat` en Linux); el auditor verificará que todos los equipos apunten a la fuente interna autorizada, que la zona horaria y marcas de tiempo sean consistentes y que el desfase temporal respecto a la fuente UTC sea nulo o esté dentro de los límites tolerados por la política.



Cláusula 8: Controles Tecnológicos

Control 8.18 Uso de programas de utilidad privilegiados

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# sistema_y_red- trabajo_seguridad # Secure_configura- ción #Aplicación_seguridad	# Proteccion

- **El Control:** El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de las aplicaciones debe ser restringido y estrictamente controlado.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en regular aquellas herramientas de software y comandos del sistema que cuentan con facultades para eludir los controles de seguridad lógicos establecidos (por ejemplo, editores de bajo nivel de disco, analizadores de paquetes de red, depuradores de memoria, herramientas de particionado, scripts de administración profunda o consolas de base de datos con comandos de bypass). Los puntos clave resumidos son:
 - Identificación e Inventario de Utilidades Críticas:** La organización debe identificar y clasificar todos los programas de utilidad y herramientas de diagnóstico capaces de modificar registros del sistema, alterar tablas de base de datos directamente o sobreescribir controles de acceso.
 - Restricción de Instalación y Ejecución:** La disponibilidad de estas herramientas en servidores de producción debe limitarse al mínimo indispensable. Deben eliminarse o deshabilitarse de las imágenes estándar de producción si no son requeridas para la operación continua.
 - Procesos de Autorización y Uso Temporal:** El uso de programas de utilidad privilegiados debe requerir una solicitud formal, justificación técnica y aprobación previa (idealmente bajo esquemas de acceso temporal o bajo demanda).
 - Segregación respecto al Software de Aplicación:** Se debe impedir que los usuarios operativos de las aplicaciones de negocio puedan invocar o acceder a programas de utilidad del sistema operativo subyacente.



Cláusula 8: Controles Tecnológicos

Control 8.18 Uso de programas de utilidad privilegiados

- **Otra Información:** La norma resalta que los programas de utilidad representan un vector de riesgo crítico tanto para incidentes internos involuntarios como para sabotaje o encubrimiento de actividades maliciosas (por ejemplo, utilidades empleadas para deshabilitar agentes de seguridad o purgar registros). Por ello, su ejecución debe estar estrictamente desvinculada de entornos productivos rutinarios.

💡 **Aplica políticas de ejecución restringida con AppLocker o WDAC:** En lugar de confiar solo en los permisos de usuario, utiliza soluciones como Windows Defender Application Control (WDAC) o políticas de Whitelisting en Linux para bloquear la ejecución no autorizada de herramientas potentes como regedit, editores hexadecimales, tcpdump en servidores productivos.

💡 **Elimina compiladores y depuradores de tus entornos de producción:** Una buena práctica de hardening consiste en purgar compiladores (como gcc), depuradores (como gdb) y utilidades de rescate/particionado de los servidores en vivo. Si un atacante o usuario no autorizado accede al servidor, no encontrará las herramientas nativas necesarias para compilar exploits o manipular la memoria.

💡 **Monitorea y graba las sesiones donde se invoquen utilidades de sistema:** Cuando un ingeniero deba utilizar una herramienta de soporte de bajo nivel o consola de mantenimiento en un sistema central, canaliza el acceso a través de una solución PAM que no solo registre los comandos ingresados, sino que grabe la sesión en video/texto para asegurar el no repudio absoluto.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Uso de Herramientas y Programas de Utilidad Privilegiados, así como el listado de utilidades autorizadas para el equipo de infraestructura y bases de datos. Para verificar el cumplimiento en la práctica, el auditor seleccionará una muestra de servidores de producción y solicitará una demostración en vivo (o revisión de configuraciones) para comprobar que los usuarios estándar y operadores no puedan invocar herramientas de administración de bajo nivel, verificando además que existan registros de autorización y bitácoras de auditoría detalladas cada vez que un administrador utilizó una utilidad crítica en un entorno productivo.



Cláusula 8: Controles Tecnológicos

Control 8.18 Uso de programas de utilidad privilegiados

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

- **El Control:** Se deben implementar procedimientos y medidas técnicas para gestionar de forma segura la instalación de software en sistemas operacionales.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en regular la incorporación de cualquier tipo de software en los sistemas productivos u operacionales para evitar la introducción de vulnerabilidades, inestabilidad en los servicios o código malicioso. Los puntos clave resumidos son:
 - Restricción de Permisos de Instalación:** Los usuarios finales y operadores no deben tener permisos administrativos ni capacidades técnicas para instalar software de forma autónoma en sus estaciones de trabajo o en servidores operacionales.
 - Proceso Formal de Evaluación y Aprobación:** Todo nuevo software o actualización debe someterse a una evaluación de seguridad previa (revisión de reputación del fabricante, licencias, compatibilidad y riesgos de ciberseguridad) y contar con una autorización formal antes de desplegarse.
 - Pruebas en Ambientes Separados:** Las actualizaciones o nuevos paquetes deben probarse rigurosamente en entornos de prueba o preproducción (staging/QA) antes de su liberación en el entorno productivo real.
 - Uso de Fuentes Confiables y Repositorios Centralizados:** Las descargas e instalaciones deben realizarse exclusivamente desde repositorios oficiales, firmados digitalmente y verificados mediante sumas de verificación (hashes como SHA-256).
 - Estrategia de Reversión (Rollback):** Antes de aplicar cualquier instalación o cambio mayor de software, se debe contar con un respaldo verificado y un plan documentado de reversión en caso de fallos imprevistos.



Cláusula 8: Controles Tecnológicos

Control 8.18 Uso de programas de utilidad privilegiados

- **Otra Información:** La norma resalta la importancia de gestionar las herramientas de desarrollo y compiladores, las cuales no deben instalarse en sistemas de producción a menos que sea estrictamente indispensable. Asimismo, en arquitecturas modernas basadas en contenedores (como Docker o Kubernetes) e infraestructura en la nube, este control se traduce en la inmutabilidad de las imágenes: no se instala software sobre contenedores en ejecución, sino que se reconstruye y despliega una nueva imagen validada a través de un canal automatizado de CI/CD.

💡 **Implementa listas blancas de aplicaciones (Application Whitelisting):** En lugar de intentar bloquear manualmente cada software malicioso conocido, utiliza herramientas como AppLocker, WDAC o soluciones de control de endpoints para definir qué ejecutables específicos están permitidos en los equipos de la organización; cualquier archivo que no esté en la lista permitida será bloqueado por defecto.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Instalación y Control de Software, junto con el Procedimiento de Gestión de Cambios de TI. Para validar el cumplimiento en la práctica, seleccionará una muestra de estaciones de trabajo y servidores de producción: en las estaciones verificará que los usuarios estándar carezcan de privilegios de administrador local para ejecutar instaladores; en los servidores comprobará que las aplicaciones instaladas coincidan con el inventario de software autorizado y pedirá las evidencias (tickets de cambio, actas de pruebas en entornos no productivos y planes de reversión) de las últimas instalaciones o actualizaciones mayores liberadas en el entorno operativo.



Cláusula 8: Controles Tecnológicos

Control 8.19 Instalación de software en sistemas operativos

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

- **El Control:** Se deben implementar procedimientos y medidas técnicas para gestionar de forma segura la instalación de software en sistemas operacionales.
- **Resumen de las Directrices de Implementación:**La guía de implementación se enfoca en regular la incorporación de aplicaciones, librerías, parches, actualizaciones o scripts en los sistemas productivos u operacionales para evitar fallos de estabilidad, incompatibilidades o la introducción de código malicioso. Los puntos clave resumidos son:
 - Restricción de Privilegios de Instalación:** Los usuarios finales y operadores no deben contar con permisos administrativos ni capacidades técnicas para instalar software de manera autónoma en estaciones de trabajo o servidores operativos.
 - Evaluación y Aprobación Previa:** Todo software, actualización o paquete de terceros debe someterse a una evaluación de seguridad (reputación del proveedor, licenciamiento, soporte y análisis de vulnerabilidades) y contar con una autorización formal antes de su despliegue.
 - Pruebas en Entornos Separados:** Las instalaciones o cambios mayores deben probarse previamente en ambientes de prueba o preproducción (QA / Staging) para validar compatibilidad y rendimiento antes de pasar a producción.
 - Fuentes Confiables y Verificación de Integridad:** La descarga y despliegue deben realizarse exclusivamente desde repositorios oficiales, firmados digitalmente y validados mediante sumas de verificación (checksums/hashes).
 - Plan de Reversión (Rollback):** Toda instalación en sistemas operativos de producción debe contar con respaldos previos y un procedimiento documentado de marcha atrás en caso de error crítico.



Cláusula 8: Controles Tecnológicos

Control 8.19 Instalación de software en sistemas operativos

- **Otra Información:** La norma resalta que las herramientas de desarrollo, compiladores y utilidades de depuración no deben instalarse en sistemas de producción. Asimismo, en arquitecturas modernas de contenedores (Docker, Kubernetes) o infraestructura en la nube, este control se gestiona bajo el principio de infraestructura inmutable: no se instala software directamente en contenedores en ejecución, sino que se construye, valida y despliega una nueva imagen inalterable a través de un canal automatizado de integración y entrega continua (CI/CD).

💡 **Implementa listas blancas de aplicaciones (Application Whitelisting):** Configura soluciones como AppLocker, Windows Defender Application Control (WDAC) o políticas de ejecución restringida en Linux para permitir únicamente ejecutables firmados por entidades confiables o alojados en rutas protegidas, bloqueando por defecto cualquier archivo ejecutable no autorizado.

💡 **Integra análisis de composición de software (SCA) en despliegues automatizados:** Si la organización utiliza pipelines de CI/CD para desplegar infraestructura o software en servidores, integra escaneos automáticos de dependencias para detectar componentes obsoletos o vulnerabilidades conocidas antes de la instalación en producción.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Instalación de Software y el Procedimiento de Control de Cambios de TI. Durante la revisión, seleccionará una muestra de estaciones de trabajo y servidores productivos: en los endpoints verificará técnicamente que los usuarios comunes no pertenezcan al grupo de administradores locales; en los servidores comprobará que las aplicaciones instaladas coincidan con el inventario de software autorizado y pedirá evidencias documentales de las últimas instalaciones o actualizaciones mayores liberadas en producción.



Cláusula 8: Controles Tecnológicos

Control 8.20 Seguridad de redes

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Detectar	# sistema_y_red- trabajo_seguridad	# Proteccion

- **El Control:** Las redes, los dispositivos de red y sus servicios deben asegurarse, gestionarse y controlarse para proteger la información en los sistemas y aplicaciones.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en proteger la infraestructura de comunicaciones interna y perimetral para salvaguardar la confidencialidad, integridad y disponibilidad del tráfico de datos que transita por ella. Los puntos clave resumidos son:
 - Gestión y Control Operativo:** La administración de dispositivos de red debe estar restringida exclusivamente a personal autorizado, utilizando canales de gestión seguros y cifrados (como SSHv2, HTTPS o VPNs dedicadas de administración).
 - Seguridad en Servicios y Protocolos de Red:** Se deben deshabilitar protocolos inseguros o en texto plano (como Telnet, FTP, HTTP, SNMPv1/v2) y reemplazarlos por sus contrapartes seguras (SSH, SFTP, HTTPS, SNMPv3).
 - Protección Perimetral y Filtrado de Tráfico:** Implementar firewalls de última generación (NGFW), sistemas de prevención de intrusiones (IPS) y pasarelas de seguridad para inspeccionar, filtrar y autorizar únicamente el tráfico de red estrictamente necesario (regla de "denegar todo por defecto").
 - Seguridad en Redes Inalámbricas (Wi-Fi):** Las redes inalámbricas corporativas deben utilizar mecanismos de autenticación y cifrado robustos (WPA3-Enterprise / 802.1X), manteniendo redes de invitados completamente aisladas del tráfico interno de la organización.
 - Monitoreo y Registro de Dispositivos de Red:** Los dispositivos de red deben enviar sus registros de eventos (syslog) y métricas de rendimiento a repositorios centralizados para detectar fallas operativas o anomalías de tráfico de forma proactiva.



Cláusula 8: Controles Tecnológicos

Control 8.20 Seguridad de redes

- **Otra Información:** La norma resalta la estrecha relación entre este control y el diseño de la arquitectura de red (como la segregación y el modelo de confianza cero o Zero Trust). Asimismo, destaca la necesidad de establecer acuerdos de nivel de servicio (SLA) y requisitos de seguridad estrictos cuando la infraestructura de red o las comunicaciones son provistas por terceros.

💡 **Aísla el plano de administración de la red:** Nunca permitas que las interfaces de administración de tus routers, switches y firewalls sean accesibles desde la misma red donde navegan los usuarios finales. Configura una VLAN de administración dedicada y aislada, a la cual solo se pueda acceder mediante estaciones de trabajo de administración seguras (PAWs) o a través de una VPN interna con MFA.

💡 **Elimina protocolos heredados y no cifrados en la red:** Realiza un escaneo interno para identificar tráfico residual inseguro. Prohíbe y bloquea en switches y firewalls protocolos antiguos como Telnet o HTTP plano para tareas de gestión o transmisión de datos internos, forzando configuraciones con TLS 1.3 y SSH con algoritmos criptográficos robustos.

💡 **Protege los puertos físicos de acceso con 802.1X:** Evita que cualquier persona conecte una laptop desconocida a una roseta de red en una sala de juntas o pasillo y obtenga acceso inmediato a la red corporativa. Implementa control de acceso a la red (NAC) basado en el estándar IEEE 802.1X para autenticar mediante certificados digitales cada dispositivo físico antes de asignarle conectividad de red.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Seguridad de Redes y los diagramas de arquitectura y topología de red actualizados. Para evaluar el control en la práctica, pedirá acceso o capturas de configuración de una muestra de dispositivos de red; el auditor verificará que no existan contraseñas por defecto, que las interfaces de gestión utilicen protocolos cifrados, que las reglas del firewall apliquen el principio de mínimo acceso que las redes Wi-Fi de invitados estén debidamente aisladas de la red corporativa y que los registros de red se estén enviando a un servidor central de bitácoras.



Cláusula 8: Controles Tecnológicos

Control 8.21 Seguridad de los servicios de red

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

- **El Control:** Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deben identificarse, implementarse y monitorearse.
- **Resumen de las Directrices de Implementación:** Mientras que el control 8.20 se enfoca en los dispositivos físicos/lógicos y la topología, el control 8.21 se centra en los servicios de conectividad y valor agregado provistos por operadores de telecomunicaciones o gestionados internamente (enlaces dedicados, MPLS, SD-WAN, DNS público/privado, pasarelas VPN, servicios de mitigación DDoS o telefonía IP). Los puntos clave resumidos son:
 - Identificación de Requisitos de Seguridad:** Se deben definir formalmente las características de seguridad exigidas para cada servicio de red, tales como cifrado en tránsito, autenticación de endpoints, redundancia y capacidad de respuesta ante fallos.
 - Acuerdos de Nivel de Servicio (SLA):** Los contratos con proveedores de telecomunicaciones deben estipular claramente métricas de disponibilidad (uptime), ancho de banda garantizado, latencia máxima tolerada, tiempos de respuesta y tiempos de restauración ante caídas (MTTR).
 - Capacidad de Auditoría y Monitoreo:** La organización debe contar con facultades para monitorear el desempeño del proveedor y recibir alertas tempranas sobre degradación del servicio o incidentes que afecten la conectividad.
 - Seguridad en Servicios Críticos Compartidos:** Se deben proteger servicios de soporte fundamentales como el DNS (para prevenir envenenamiento de caché mediante DNSSEC) y las conexiones remotas a través de túneles VPN cifrados punto a punto.



Cláusula 8: Controles Tecnológicos

Control 8.21 Seguridad de los servicios de red

- **Otra Información:** La norma resalta que, ante la adopción de esquemas híbridos y de nube, la interconexión entre centros de datos y proveedores cloud (por ejemplo, AWS Direct Connect o Azure ExpressRoute) debe tratarse bajo este control. Además, es indispensable verificar que los proveedores de servicios de red cuenten con certificaciones de seguridad reconocidas (como ISO/IEC 27001 o SOC 2) y planes probados de continuidad del negocio.

💡 **Protege la infraestructura DNS con DNSSEC y filtrado recursivo:** El servicio de resolución de nombres (DNS) es la columna vertebral de toda tu conectividad. Implementa DNS Security Extensions (DNSSEC) para evitar la suplantación de dominios y utiliza servicios de filtrado DNS empresarial (como Cisco Umbrella o Cloudflare Gateway) para bloquear en tiempo real peticiones hacia dominios maliciosos conocidos antes de que se establezca la conexión.

💡 **Audita los SLAs de tus enlaces con monitoreo sintético independiente:** Configura herramientas de monitoreo sintético (como Prometheus Blackbox Exporter o PRTG) que envíen paquetes de prueba continuos a través de tus enlaces para medir disponibilidad y pérdida de paquetes real; si el ISP incumple los SLAs pactados, tendrás datos duros para exigir penalizaciones comerciales.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el catálogo o inventario de servicios de red contratados (enlaces de internet, VPNs corporativas, servicios gestionados de DNS o SD-WAN) y los contratos vigentes con los proveedores de telecomunicaciones. Para evaluar el control, revisará que dichos contratos incluyan cláusulas formales de seguridad de la información, confidencialidad y acuerdos de nivel de servicio (SLAs) claros; posteriormente, pedirá los tableros o reportes mensuales de monitoreo del rendimiento y disponibilidad de dichos servicios para verificar que la organización supervisa activamente que los proveedores cumplan con los parámetros técnicos pactados y gestiona adecuadamente cualquier desviación o incidente de conectividad reportado.



Cláusula 8: Controles Tecnológicos

Control 8.22 Segregación de redes

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

- **El Control:** Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes.
- **Resumen de las Directrices de Implementación:**La guía de implementación se enfoca en dividir una red corporativa en zonas de seguridad lógicas o físicas independientes para contener incidentes, mitigar el movimiento lateral de posibles atacantes y limitar el acceso no autorizado a los sistemas más críticos. Los puntos clave resumidos son:
 - Criterios de Segmentación:** La segregación de la red debe basarse en la clasificación de la información, criticidad de los activos, funciones organizacionales (ej. Recursos Humanos, Finanzas) y requisitos regulatorios.
 - Mecanismos Técnicos de Segregación:**
 - VLANs y Subredes: División lógica del tráfico en la capa 2 y capa 3 del modelo OSI.
 - Zonas Desmilitarizadas (DMZ): Aislamiento de servidores públicos o expuestos a internet (como servidores web corporativos) de las redes internas.
 - Firewalls y Pasarelas de Control: Filtrado e inspección de tráfico entre segmentos para autorizar únicamente puertos y protocolos indispensables.
 - Separación de Entornos:** Los entornos de desarrollo, pruebas/homologación y producción deben residir en segmentos de red totalmente aislados entre sí.
 - Aislamiento de Tecnologías Específicas:** Dispositivos IoT, redes Wi-Fi de invitados y componentes de videovigilancia/control de acceso físico deben estar confinados en segmentos de red independientes sin acceso a los servidores principales del negocio.



Cláusula 8: Controles Tecnológicos

Control 8.22 Segregación de redes

- **Otra Información:** La norma resalta la adopción de arquitecturas modernas de Microsegmentación y principios de Confianza Cero (Zero Trust Network Architecture - ZTNA). A diferencia de la segmentación perimetral tradicional (que confía en cualquier dispositivo una vez dentro de la red interna), la microsegmentación permite aplicar políticas de seguridad granulares a nivel de carga de trabajo (workload) individual o contenedor, evitando que la vulneración de una máquina comprometa a los demás equipos de su mismo segmento.

💡 **Aísla por completo los dispositivos IoT e impresoras:** Confinarlos en una VLAN dedicada de "IoT" sin visibilidad hacia tus servidores de bases de datos o controladores de dominio cerrará la puerta a una de las vías de pivoteo más comunes usadas por los ciberdelincuentes.

💡 **Implementa una DMZ real de doble firewall para servicios públicos:** Si publicas servicios hacia internet (como portales de clientes o APIs), nunca conectes esos servidores directamente a la red LAN interna. Diseña una Zona Desmilitarizada (DMZ) donde el servidor web intermedio reciba las solicitudes de internet y únicamente tenga permitido hablar con la base de datos interna mediante un puerto estricto y específico a través de un segundo firewall interno.

💡 **Elimina la red "plana" y adopta microsegmentación:** Deshabilita la comunicación horizontal entre estaciones de trabajo (mediante aislamiento de puertos o reglas de software en el endpoint), obligando a que todo el tráfico pase por inspección y control centralizado.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Segregación de Redes y el Diagrama de Arquitectura de Red y Zonas de Seguridad actualizado. Para verificar la efectividad técnica del control, el auditor revisará la configuración de los firewalls internos y switches de distribución, prestando especial atención a las reglas que conectan las diferentes zonas; comprobará que exista un aislamiento real entre los entornos de desarrollo y producción, validará que las redes Wi-Fi para visitantes no tengan ruta de acceso a los servidores corporativos y pedirá evidencia de pruebas de escaneo o penetración que demuestren que no es posible alcanzar zonas de alta confidencialidad desde segmentos no autorizados.



Cláusula 8: Controles Tecnológicos

Control 8.23 Filtrado Web

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

- **El Control:** El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en regular la navegación web saliente del personal y los sistemas para prevenir infecciones por malware, ataques de phishing y el uso indebido de recursos de red. Los puntos clave resumidos son:
 - Bloqueo Basado en Categorías y Reputación:** Restringir el acceso a sitios web clasificados como peligrosos (dominios recién registrados, phishing, malware, juegos de azar o contenido para adultos).
 - Inspección de Tráfico Cifrado (SSL/TLS Inspection):** Descifrar e inspeccionar selectivamente el tráfico HTTPS saliente para detectar amenazas ocultas en canales seguros.
 - Control de Descargas:** Impedir la descarga de tipos de archivos de alto riesgo (como ejecutables .exe, .scr, scripts .bat o macros) desde sitios no confiables.
 - Protección Fuera de la Red Corporativa:** Extender las políticas de filtrado web hacia los equipos portátiles cuando los empleados trabajan de forma remota o fuera de la oficina.



Cláusula 8: Controles Tecnológicos

Control 8.23 Filtrado Web

Otra Información :La norma resalta que el filtrado web también previene la fuga no autorizada de datos (Shadow IT), al bloquear la subida de documentos a servicios de almacenamiento personal en la nube. Asimismo, aconseja complementar los bloqueos automáticos con mensajes claros en el navegador que expliquen al usuario por qué el sitio fue denegado y cómo solicitar una excepción justificada por el negocio.

💡 **Bloquea automáticamente dominios recién creados:** Configura tu pasarela web para vetar sitios registrados hace menos de 30 días, ya que los atacantes usan dominios efímeros para campañas de phishing antes de que sean catalogados como maliciosos.

💡 **Extiende el agente web al endpoint remoto:** No limites el filtrado al firewall del edificio. Instala agentes de seguridad web o DNS (ej. Cisco Umbrella o Cloudflare WARP) directamente en las laptops para mantener las restricciones activas en teletrabajo.

💡 **Habilita inspección HTTPS selectiva:** El 90% del tráfico web viaja cifrado. Despliega inspección SSL en tu proxy/firewall para auditar descargas sospechosas, exceptuando únicamente categorías sensibles como banca en línea y salud por temas de privacidad.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Uso Aceptable de Internet y la Política de Filtrado Web. Durante la revisión técnica, verificará en la consola de administración (Proxy, Firewall o SWG) las categorías de sitios bloqueadas, las listas de excepciones autorizadas y las reglas de inspección de tráfico seguro; asimismo, solicitará reportes de navegación e intentos de acceso bloqueados hacia sitios maliciosos para comprobar que las herramientas restringen efectivamente el tráfico web no deseado tanto dentro como fuera de la red local.



Cláusula 8: Controles Tecnológicos

Control 8.24 Uso de Criptografia

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

El Control: Se deben definir e implementar reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

- **Resumen de las Directrices de Implementación:**La guía de implementación se enfoca en establecer los principios y mecanismos técnicos para garantizar la confidencialidad, autenticidad, integridad y no repudio de la información mediante el uso correcto de algoritmos y la administración de su ciclo de vida. Los puntos clave resumidos son:
 - Política de Criptografía:** Establecer lineamientos formales que definan qué datos deben cifrarse, los algoritmos y longitudes de clave permitidos, y las herramientas autorizadas.
 - Cifrado en Reposo y en Tránsito:** Aplicar algoritmos robustos tanto para datos almacenados como para datos transmitidos por redes públicas o internas (TLS, IPsec, SSH).
 - Gestión del Ciclo de Vida de Claves Criptográficas:** Definir procesos seguros para la generación, almacenamiento, distribución, rotación, revocación y destrucción de llaves criptográficas.
 - Protección de Llaves Privadas y Secretas:** Custodiar las claves contra accesos no autorizados mediante módulos de seguridad de hardware (HSM), almacenes dedicados de claves (KMS) o controles de acceso basados en roles.



Cláusula 8: Controles Tecnológicos

Control 8.24 Uso de Criptografia

- **Otra Información** :La norma resalta la importancia de la agilidad criptográfica (cryptographic agility), es decir, la capacidad de la organización para reemplazar algoritmos o aumentar la longitud de claves rápidamente cuando un estándar quede obsoleto o vulnerable (como ocurrió con DES, MD5, SHA-1 o TLS 1.0/1.1). Además, advierte sobre el impacto de las leyes locales respecto a la importación, exportación y uso de tecnologías de cifrado en diferentes jurisdicciones.

💡 **Prohíbe algoritmos y suites criptográficas obsoletas:** Retira de inmediato el soporte para TLS 1.0/1.1, SSLv3, 3DES, RC4, MD5 y SHA-1 en todos tus servicios web y conexiones internas, forzando TLS 1.3/1.2 y AES-256 o ChaCha20.

💡 **Centraliza la custodia de claves en servicios KMS o HSM:** Evita guardar contraseñas o llaves privadas en archivos de configuración o código fuente plano. Utiliza administradores dedicados con políticas de acceso de privilegio mínimo.

💡 **Automatiza la rotación de certificados y llaves:** Implementa herramientas con protocolo ACME (como cert-manager o Let's Encrypt) para renovar certificados digitales y llaves TLS automáticamente antes de su vencimiento, evitando caídas de servicio por certificados caducados.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Criptografía y Gestión de Claves Criptográficas de la organización. Para comprobar su cumplimiento técnico, inspeccionará la configuración de servidores y servicios expuestos (por ejemplo, validando los protocolos y suites de cifrado habilitados con escaneos tipo SSL Labs); asimismo, verificará cómo se almacenan las llaves privadas de los certificados y credenciales de bases de datos, solicitando evidencia de los procedimientos de generación, rotación periódica y revocación de llaves, así como la separación entre los custodios de las claves y los administradores de los sistemas que procesan los datos cifrados.



Cláusula 8: Controles Tecnológicos

Control 8.25 Ciclo de vida de desarrollo seguro

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

- **El Control:** Se deben establecer y aplicar reglas para el desarrollo seguro de software y sistemas.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en integrar la seguridad en cada una de las fases del ciclo de vida del desarrollo de software (SSDLC / Secure Software Development Life Cycle), abarcando tanto el desarrollo interno como el contratado a terceros. Los puntos clave resumidos son:
 - Seguridad desde el Diseño (Security by Design):** Incorporar requerimientos de seguridad y modelado de amenazas (threat modeling) desde la fase de planeación y arquitectura antes de escribir código.
 - Estándares de Codificación Segura:** Definir directrices técnicas obligatorias para los desarrolladores que mitiguen vulnerabilidades comunes (como las listadas en OWASP Top 10 o CWE/SANS Top 25).
 - Seguridad en Entornos de Desarrollo:** Proteger los repositorios de código, entornos de compilación (build pipelines) y herramientas de CI/CD con controles de acceso estrictos y autenticación multifactor (MFA).
 - Pruebas de Seguridad Continuas:** Integrar pruebas estáticas (SAST), dinámicas (DAST) y análisis de dependencias de terceros (SCA) a lo largo del proceso de desarrollo.
 - Separación de Funciones y Control de Versiones:** Mantener segregados los entornos de desarrollo, pruebas y producción, impidiendo que los desarrolladores desplieguen cambios directamente a producción sin una revisión formal entre pares (code review).



Cláusula 8: Controles Tecnológicos

Control 8.25 Ciclo de vida de desarrollo seguro

- **Otra Información:** La norma destaca que este control aplica independientemente de la metodología de trabajo (Ágil, Scrum, DevOps, Cascada) y promueve la adopción de prácticas DevSecOps, donde la seguridad se automatiza dentro de los canales de integración continua para no frenar la velocidad de entrega del negocio.

💡 **Integra herramientas SAST y SCA en tus pipelines de CI/CD:** Automatiza el análisis de código estático (ej. SonarQube) y el escaneo de librerías vulnerables (ej. Snyk o Trivy) para romper la compilación (break the build) si se detecta un fallo crítico antes de fusionar ramas.

💡 **Capacita a los desarrolladores en directrices OWASP:** El software no se hace seguro con parches de último minuto; entrena periódicamente a tus programadores en codificación defensiva contra inyecciones SQL, XSS y gestión incorrecta de sesiones.

💡 **Aplica revisión de código por pares (Peer Review) obligatoria:** Configura tus repositorios (GitHub, GitLab, Azure DevOps) con políticas de ramas protegidas (Branch Protection Rules) que exijan al menos una aprobación formal y pruebas automatizadas superadas antes de aceptar un Pull Request hacia la rama principal.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política y la Guía de Estándares de Desarrollo Seguro de Software (SSDLC). Durante la revisión, seleccionará un proyecto o aplicación reciente y revisará la evidencia de cada etapa: el análisis de requerimientos de seguridad inicial, la configuración de los repositorios y flujos de CI/CD para comprobar las reglas de ramas protegidas, los reportes de escaneo de vulnerabilidades automáticos (SAST/DAST) generados durante la compilación, y los registros de aprobación formal de los Pull Requests previos al paso a producción.



Cláusula 8: Controles Tecnológicos

Control 8.26 Requisitos de seguridad de la aplicación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # sistema_y_red- trabajo_seguridad	# Proteccion # Defensa

- **El Control:** Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar que los criterios de seguridad no se consideren como un parche de última hora, sino como especificaciones funcionales y no funcionales obligatorias desde la concepción del software, ya sea mediante desarrollo interno, subcontratación o compra de soluciones comerciales (COTS/SaaS). Los puntos clave resumidos son:
 - Identificación del Nivel de Confianza y Criticidad:** Evaluar el tipo de datos que procesará la aplicación (PII, datos financieros, secretos comerciales) y su impacto en el negocio para definir el nivel de protección requerido.
 - Aprobación Formal:** Los requerimientos de seguridad deben ser validados y aprobados formalmente por los propietarios del sistema y el equipo de seguridad antes de iniciar la construcción o contratación.



Cláusula 8: Controles Tecnológicos

Control 8.26 Requisitos de seguridad de la aplicación

- **Otra Información:** La norma destaca la importancia de contemplar aspectos regulatorios y de privacidad (como GDPR, regulaciones bancarias o normativas locales de protección de datos) al redactar las especificaciones. Asimismo, subraya que los requisitos de seguridad deben mantenerse actualizados durante todo el ciclo de vida de la aplicación conforme evolucionan las amenazas del entorno.

💡 **Integra historias de usuario de seguridad (Abuser Stories):** En tus tableros ágiles (Jira o Azure Boards), incluye casos de abuso junto a los requisitos funcionales para definir claramente cómo debe reaccionar el sistema ante intentos de manipulación o accesos no autorizados.

💡 **Usa listas de verificación basadas en ASVS de OWASP:** Adopta el Application Security Verification Standard (ASVS) como marco de referencia para redactar requisitos técnicos estandarizados, evitando especificaciones ambiguas tanto para tus desarrolladores como para proveedores externos.

💡 **Establece un cuestionario de seguridad obligatorio para adquisiciones de software:** Ninguna compra de software o contratación de SaaS debe concretarse sin una evaluación previa del equipo de ciberseguridad que valide esquemas de cifrado, soporte de SSO/MFA y políticas de respaldo del proveedor.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Requisitos de Seguridad de Aplicaciones y los documentos de especificación técnica o arquitectura de proyectos recientes (tanto de desarrollo interno como de adquisiciones comerciales). Durante la revisión, comprobará que existan matrices de requisitos de seguridad aprobadas formalmente antes del inicio del desarrollo o compra; asimismo, verificará cómo se definieron controles específicos de autenticación, cifrado y trazabilidad, y solicitará evidencia del cumplimiento de dichos requisitos en las actas de aceptación final de los sistemas evaluados.



Cláusula 8: Controles Tecnológicos

Control 8.27 Arquitectura del sistema seguro y principios de ingeniería

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

- **El Control:** Los principios para la ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en establecer los fundamentos estructurales y patrones de diseño técnico para que los sistemas de información sean resilientes, modulares y seguros desde su arquitectura base. Los puntos clave resumidos son:
 - Adopción de Principios Fundamentales de Ingeniería:** Aplicar conceptos clásicos y modernos de seguridad de sistemas, tales como:
 - Defensa en profundidad (Defense in Depth): Implementar múltiples capas de control superpuestas para que el fallo de una barrera no comprometa todo el entorno.
 - Menor privilegio y superficie de ataque mínima: Limitar accesos, puertos, servicios y componentes a lo estrictamente indispensable.
 - Fallo seguro (Fail-Safe Defaults): Configurar los sistemas para que, ante un error o excepción no controlada, el estado resultante sea de bloqueo y no de acceso abierto.
 - Modularidad y Aislamiento:** Diseñar arquitecturas divididas en componentes desacoplados para evitar que la vulneración de un módulo afecte al resto del sistema.
 - Mantenimiento y Evolución Arquitectónica:** Actualizar y revisar periódicamente las pautas de arquitectura para adaptarlas a nuevas tecnologías (nube, microservicios, contenedores) y vectores de ataque emergentes.



Cláusula 8: Controles Tecnológicos

Control 8.27 Arquitectura del sistema seguro y principios de ingeniería

- **Otra Información:** La norma resalta que estos principios de ingeniería aplican a todas las capas del sistema: infraestructura, redes, sistemas operativos, bases de datos, APIs y lógica de negocio. Además, deben integrarse en los procesos de compras de tecnología para garantizar que las soluciones adquiridas a terceros se acoplen armónicamente a los patrones arquitectónicos de la empresa.

💡 **Estandariza patrones arquitectónicos seguros:** Define plantillas de referencia (ej. arquitecturas de microservicios con API Gateways y autenticación delegada vía OAuth 2.0/OIDC) para que los equipos de desarrollo no diseñen esquemas propios desde cero.

💡 **Aplica desacoplamiento y menor superficie de exposición:** Evita arquitecturas monolíticas donde la base de datos esté expuesta directamente a la capa de presentación; utiliza capas intermedias de servicios y zonas desmilitarizadas internas.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el documento formal de Principios y Estándares de Arquitectura e Ingeniería Segura de la organización. Para evaluar su aplicación real, revisará los diagramas de arquitectura técnica y modelos de amenazas (Threat Models) de proyectos representativos; constatará que se hayan aplicado capas de defensa en profundidad, patrones de fallo seguro y segregación de componentes, y solicitará evidencia de que el comité o líder de arquitectura de seguridad evaluó y aprobó formalmente el diseño técnico antes de la fase de construcción.



Cláusula 8: Controles Tecnológicos

Control 8.28 Codificación segura

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

- **El Control:** Los principios de codificación segura deben aplicarse al desarrollo de software.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en las prácticas concretas de escritura de código fuente para evitar la introducción de fallos, malas prácticas y vulnerabilidades explotables durante la programación. Los puntos clave resumidos son:
 - Estándares y Guías de Codificación:** Definir y aplicar guías de estilo y buenas prácticas de desarrollo seguro específicas para cada lenguaje de programación utilizado en la organización (ej. directrices contra inyecciones SQL, Cross-Site Scripting, desbordamientos de búfer o deserialización insegura).
 - Validación y Sanitización de Datos:** Implementar validación estricta de entradas (tipo de dato, longitud, formato mediante listas blancas) y codificación/escape contextual de salidas para evitar ataques de inyección.
 - Manejo Seguro de Errores y Excepciones:** Evitar que los mensajes de error devueltos a los usuarios expongan información técnica interna (como volcados de memoria, consultas SQL o rutas del servidor).
 - Gestión de Secretos y Credenciales:** Prohibir terminantemente la inclusión de contraseñas, tokens de API o claves criptográficas directamente en el código fuente (hardcoded secrets).
 - Revisión y Refactorización Continua:** Realizar revisiones de código estático y refactorización periódica para eliminar código muerto (dead code), librerías en desuso y componentes vulnerables.



Cláusula 8: Controles Tecnológicos

Control 8.28 Codificación segura

- **Otra Información:** La norma destaca la importancia de consultar catálogos de vulnerabilidades reconocidos internacionalmente, tales como el CWE/SANS Top 25 y el OWASP Top 10, así como las guías del SEI CERT Coding Standards. Asimismo, subraya que las prácticas de codificación segura aplican por igual a componentes desarrollados internamente, scripts de automatización, infraestructura como código (IaC) y librerías de código abierto (open source).

💡 **Implementa escáneres de secretos en pre-commit:** Configura herramientas como TruffleHog o Git-secrets en los entornos locales de los desarrolladores para bloquear automáticamente los commits que contengan accidentalmente API keys, tokens o contraseñas en texto plano.

💡 **Usa consultas parametrizadas (Prepared Statements) por defecto:** Elimina por completo la concatenación manual de cadenas en consultas SQL o llamadas al sistema para neutralizar de raíz los ataques de inyección.

💡 **Estandariza el manejo de excepciones:** Crea manejadores globales de errores que capturen excepciones imprevistas, registren el detalle técnico completo en la bitácora interna y muestren al usuario final únicamente un mensaje genérico y seguro.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Guía de Estándares de Codificación Segura formalizada por la organización para cada lenguaje en uso. Para validar su cumplimiento práctico, seleccionará repositorios de código al azar y revisará la configuración de las reglas de análisis estático (SAST), la ausencia de credenciales embebidas en el historial de Git, y las bitácoras de revisión de Pull Requests para comprobar que los revisores validan activamente que el código nuevo cumple con los lineamientos de seguridad antes de fusionarse a las ramas productivas.



Cláusula 8: Controles Tecnológicos

Control 8.29 Pruebas de seguridad en desarrollo y aceptación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	#Aplicación_seguridad # Information_security_assurance # sistema_y_red-trabajo_seguridad	# Proteccion

- **El Control:** Los procesos de pruebas de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en verificar y validar que las medidas de seguridad del software y de los sistemas funcionen adecuadamente y que no existan vulnerabilidades antes de su puesta en producción. Los puntos clave resumidos son:
 - Enfoque Multifacético de Pruebas:** Ejecutar distintos tipos de evaluaciones de seguridad a lo largo del ciclo de vida, incluyendo:
 - Pruebas de seguridad de aplicaciones estáticas (SAST) en el código fuente.
 - Pruebas de seguridad de aplicaciones dinámicas (DAST) en aplicaciones en ejecución.
 - Pruebas de seguridad de aplicaciones interactivas (IAST) y análisis de composición de software (SCA).
 - Pruebas de penetración (pentesting) y evaluaciones de vulnerabilidades.
 - Criterios de Aceptación Formal:** Definir umbrales mínimos de seguridad y calidad técnica como condición obligatoria para aprobar el paso de un sistema a producción.
 - Pruebas de Funcionalidades de Seguridad:** Comprobar rigurosamente que los controles lógicos (autenticación, autorización, cifrado, control de sesiones y manejo de errores) actúen según lo diseñado bajo escenarios normales y anómalos.
 - Pruebas de Estrés y Resiliencia:** Evaluar el comportamiento del sistema ante cargas extremas, ataques de denegación de servicio (DoS) o entradas de datos masivas/malformadas (fuzzing).



Cláusula 8: Controles Tecnológicos

Control 8.29 Pruebas de seguridad en desarrollo y aceptación

- **Otra Información:** La norma destaca que las pruebas deben realizarse en entornos de prueba dedicados que repliquen fielmente las características del entorno de producción, pero sin exponer datos reales sensibles (en línea con los controles 8.11 y 8.31). Asimismo, se recomienda que las pruebas de aceptación finales sean realizadas o validadas por personal independiente al equipo directo de desarrollo.

💡 **Establece Quality Gates de seguridad en CI/CD:** Configura tu canal de despliegue automatizado para detener el paso a producción si el análisis estático o de librerías detecta fallos de severidad alta o crítica sin resolver.

💡 **Automatiza pruebas dinámicas (DAST) en entornos de Staging:** Ejecuta escaneos automatizados de caja negra (ej. OWASP ZAP) contra la aplicación levantada en el ambiente de pruebas antes de cada pase mayor a producción.

💡 **Exige pruebas de penetración previas al lanzamiento:** Para sistemas críticos o expuestos a internet, contrata o ejecuta un pentest por un equipo independiente y condiciona el despliegue final al cierre de las brechas detectadas.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el Procedimiento de Pruebas de Seguridad y Criterios de Aceptación de Sistemas. Para validar el cumplimiento, seleccionará una muestra de proyectos o lanzamientos recientes a producción y revisará los reportes técnicos de análisis de vulnerabilidades (SAST/DAST) y pruebas de penetración generados durante la fase de aceptación; comprobará que los hallazgos críticos fueron remediados antes de la liberación y exigirá las actas o registros de aprobación formal de paso a producción firmadas por el responsable de seguridad o dueño del sistema.



Cláusula 8: Controles Tecnológicos

Control 8.30 Desarrollo subcontratado

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger # Detectar	# Sistema_y_red_ seguridad #Aplicación_seguridad #Proveedores_relaciones_seguridad	# Gobernanza_y_ Ecosistema # Proteccion

- **El Control:** La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratado.
- **Resumen de las Directrices de Implementación:**La guía de implementación se enfoca en asegurar que el software desarrollado, modificado o mantenido por proveedores externos (terceros, agencias de software o desarrolladores freelance) cumpla con los mismos estándares de seguridad exigidos para el desarrollo interno. Los puntos clave resumidos son:
 - Acuerdos Contractuales y Requisitos de Seguridad:** Establecer en los contratos los estándares obligatorios de codificación segura, modelos de licenciamiento, propiedad intelectual del código fuente y acuerdos de confidencialidad (NDA).
 - Supervisión y Gobernanza Continua:** Monitorear el progreso del desarrollo mediante entregables periódicos, auditorías de proceso y revisiones conjuntas de arquitectura.
 - Criterios de Aceptación y Pruebas Independientes:** Exigir reportes de pruebas de seguridad al proveedor y realizar validaciones técnicas independientes (SAST, DAST, SCA y pruebas de penetración) antes de aceptar cualquier entrega de código.
 - Custodia del Código y Depósito en Garantía (Software Escrow):** Definir quién almacena el código fuente y, si aplica, establecer acuerdos de escrow para garantizar la continuidad operativa si el proveedor quiebra o cesa operaciones.
 - Derecho de Auditoría:** Incluir cláusulas contractuales que permitan a la organización (o a auditores designados) inspeccionar las prácticas y entornos de seguridad utilizados por el desarrollador externo.



Cláusula 8: Controles Tecnológicos

Control 8.30 Desarrollo subcontratado

- **Otra Información:** La norma destaca el riesgo asociado a la cadena de suministro de software (Software Supply Chain). Los proveedores externos pueden introducir intencional o accidentalmente puertas traseras (backdoors), código malicioso o librerías de código abierto vulnerables y sin soporte. Por ello, la organización que contrata mantiene la responsabilidad legal y de seguridad sobre el producto final,

💡 **Incluye un Anexo Técnico de Seguridad en los contratos:** No dejes la seguridad a la libre interpretación del proveedor; anexa al contrato requisitos obligatorios como cumplimiento de OWASP Top 10, prohibición de credenciales embebidas y entrega de diagramas de arquitectura.

💡 **Audita el código entregado con tus propias herramientas:** Nunca aceptes un software basándote únicamente en la palabra o reportes del proveedor. Pasa el código entregado por tus propios escáneres estáticos (SAST) y análisis de dependencias (SCA) antes de realizar el pago o recepción final.

💡 **Exige el inventario de componentes (SBOM):** Solicita al proveedor una Lista de Materiales de Software (Software Bill of Materials) detallando todas las librerías de terceros y de código abierto utilizadas, sus versiones y sus licencias para monitorear vulnerabilidades futuras.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Desarrollo Subcontratado y una muestra de contratos de desarrollo de software firmados con terceros. Para validar el cumplimiento, revisará que los contratos contengan cláusulas explícitas de seguridad, derechos de propiedad intelectual y acuerdos de nivel de servicio (SLAs); asimismo, pedirá las evidencias de las revisiones de seguridad técnicas (escaneos de vulnerabilidades, pentests o revisiones de código) realizadas sobre los entregables del proveedor antes de su aprobación y puesta en producción.



Cláusula 8: Controles Tecnológicos

Control 8.31 Separación de los entornos de desarrollo, prueba y producción

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

- **El Control:** Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en establecer barreras lógicas, físicas y operativas entre los distintos ambientes para evitar que actividades de programación, pruebas inestables o accesos no autorizados afecten la confidencialidad, integridad o disponibilidad de los servicios en producción. Los puntos clave resumidos son:
 - Separación de Infraestructura y Redes:** Aislar los entornos mediante servidores independientes, cuentas/suscripciones cloud segregadas, clusters dedicados o VLANs/subredes sin enrutamiento directo indebido hacia producción.
 - Segregación de Accesos y Funciones (SoD):** Restringir los permisos de acceso de modo que el personal de desarrollo y pruebas no cuente con credenciales administrativas ni capacidad de despliegue directo sobre el ambiente productivo.
 - Flujos de Promoción Controlados:** Definir procesos formales de paso a producción a través de herramientas de integración y entrega continua (CI/CD) o equipos de operaciones independientes, basados en aprobaciones documentadas.
 - Protección de Datos Sensibles:** Prohibir el uso de bases de datos de producción con información confidencial o datos personales en entornos de desarrollo y prueba, aplicando técnicas de enmascaramiento, anonimización o generación de datos sintéticos (en concordancia con los controles 8.11 y 8.33).
 - Configuración y Parcheo Homogéneo:** Mantener los entornos de prueba lo más alineados posible con la arquitectura y configuración de producción para asegurar la validez de los resultados antes de la liberación.



Cláusula 8: Controles Tecnológicos

Control 8.31 Separación de los entornos de desarrollo, prueba y producción

- **Otra Información:** La norma resalta que, en infraestructuras modernas de nube y metodologías DevOps, la separación tradicional basada en servidores físicos se gestiona mediante arquitecturas multi-cuenta (por ejemplo, organizaciones independientes en AWS/Azure/GCP) y pipelines de automatización inmutables. Asimismo, subraya que las herramientas de desarrollo, compiladores y utilidades de depuración deben residir exclusivamente en los entornos de desarrollo y quedar vetadas de las instancias de producción.

💡 **Aísla mediante cuentas o suscripciones cloud independientes:** Evita compartir una sola cuenta para todo; crea proyectos o suscripciones separadas para desarrollo, testing y producción con políticas de identidad (IAM) y redes virtuales totalmente desvinculadas.

💡 **Revoca permisos de escritura en producción a los desarrolladores:** Implementa el principio de menor privilegio retirando accesos directos a servidores y bases de datos productivas, canalizando todos los cambios exclusivamente mediante pipelines de CI/CD automatizados.

💡 **Sintetiza o anonimiza siempre los datos de prueba:** Nunca restaures un respaldo completo de la base de datos de clientes en el entorno de desarrollo; aplica scripts de ofuscación o herramientas de datos sintéticos para proteger información personal y sensible.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Separación de Entornos y los diagramas de arquitectura de red e infraestructura que ilustren el aislamiento entre desarrollo, pruebas y producción. Para verificar el control en la práctica, seleccionará una muestra de usuarios y validará la matriz de roles y accesos para comprobar que los desarrolladores no tengan privilegios administrativos en producción; asimismo, inspeccionará los flujos de CI/CD para verificar la existencia de compuertas de aprobación (approval gates) y revisará que las bases de datos de prueba no contengan registros reales con datos personales o sensibles.



Cláusula 8: Controles Tecnológicos

Control 8.32 Gestión de cambios

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

- **El Control:** Los cambios en las instalaciones de procesamiento de información y en los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en controlar, evaluar y autorizar cualquier modificación en el hardware, software, configuraciones, redes, procesos o instalaciones de TI para evitar caídas imprevistas de servicio o brechas de seguridad. Los puntos clave resumidos son:
 - Clasificación del Cambio:** Categorizar los cambios según su nivel de impacto y urgencia.
 - Evaluación de Riesgos e Impacto:** Analizar previamente el impacto técnico, de seguridad y de negocio que provocará la modificación propuesta.
 - Flujos de Aprobación Formal:** Someter los cambios a la autorización de un comité evaluador (como el Change Advisory Board - CAB) o los dueños de los sistemas antes de su ejecución.
 - Pruebas Previas y Plan de Reversión (Rollback):** Validar la modificación en un entorno de pruebas no productivo y contar con un plan documentado y probado de marcha atrás en caso de fallo.
 - Gestión de Cambios de Emergencia:** Establecer un protocolo ágil para incidentes críticos que permita aplicar soluciones inmediatas, garantizando una revisión y documentación formal posterior



Cláusula 8: Controles Tecnológicos

Control 8.32 Gestión de cambios

- **Otra Información:** La norma resalta que la gestión de cambios debe integrarse armónicamente con metodologías modernas como DevSecOps e Infraestructura como Código (IaC). En estos entornos, las solicitudes de cambio no requieren burocracia manual lenta, sino que se gestionan como Pull Requests con pruebas automatizadas y trazabilidad completa en el historial de Git, manteniendo la gobernanza sin frenar la agilidad operativa.

💡 **Prohíbe cambios directos "en caliente" sobre producción:** Bloquea la edición manual de configuraciones o código directamente en servidores productivos; cualquier ajuste debe gestionarse mediante tickets de cambio y pipelines versionados.

💡 **Audita y limita el procedimiento de cambios de emergencia:** Diseña un flujo simplificado para contingencias reales, pero exige el registro del ticket y la revisión formal del CAB en un plazo máximo de 24 a 48 horas tras el incidente.

💡 **Condiciona la aprobación al plan de reversión probado:** No apruebes ninguna solicitud de cambio que no incluya los pasos exactos, tiempos estimados y mecanismos de respaldo necesarios para regresar al estado previo ante un fallo.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política y el Procedimiento de Gestión de Cambios de TI. Durante la auditoría, seleccionará una muestra aleatoria de cambios ejecutados en los últimos meses (normales, estándar y de emergencia) y revisará en la herramienta de mesa de ayuda (Jira, ServiceNow, GLPI) que cada solicitud cuente con su análisis de impacto, actas de pruebas en ambientes de homologación, plan de rollback, aprobación formal previa a la ventana de mantenimiento y registro de cierre exitoso; además, contrastará las bitácoras del sistema con los tickets para asegurarse de que no se realizaron modificaciones no autorizadas en producción.



Cláusula 8: Controles Tecnológicos

Control 8.32 Gestión de cambios

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

- **El Control:** Los cambios en las instalaciones de procesamiento de información y en los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en controlar, evaluar y autorizar cualquier modificación en el hardware, software, configuraciones, redes, procesos o instalaciones de TI para evitar caídas imprevistas de servicio o brechas de seguridad. Los puntos clave resumidos son:
 - Clasificación del Cambio:** Categorizar las modificaciones según su nivel de impacto y urgencia.
 - Evaluación de Riesgos e Impacto:** Analizar previamente las implicaciones técnicas, de seguridad y de negocio que provocará la modificación propuesta.
 - Flujos de Aprobación Formal:** Someter los cambios a la autorización de un comité evaluador (como el Change Advisory Board - CAB) o los propietarios de los sistemas antes de su ejecución.
 - Pruebas Previas y Plan de Reversión (Rollback):** Validar la modificación en un entorno de pruebas no productivo y contar con un procedimiento documentado y probado de marcha atrás en caso de fallo.
 - Gestión de Cambios de Emergencia:** Establecer un protocolo ágil para incidentes críticos que permita aplicar soluciones inmediatas, asegurando una revisión y documentación formal posterior.



Cláusula 8: Controles Tecnológicos

Control 8.32 Gestión de cambios

- **Otra Información:** La norma resalta que la gestión de cambios debe integrarse armónicamente con metodologías modernas como DevSecOps e Infraestructura como Código (IaC). En estos entornos, las solicitudes de cambio no requieren burocracia manual lenta, sino que se gestionan como Pull Requests con pruebas automatizadas y trazabilidad completa en el historial de Git, manteniendo la gobernanza sin frenar la agilidad operativa.

💡 **Prohíbe cambios directos "en caliente" sobre producción:** Bloquea la edición manual de configuraciones o código directamente en servidores productivos; cualquier ajuste debe gestionarse mediante tickets de cambio y repositorios versionados.

💡 **Audita y limita el procedimiento de cambios de emergencia:** Diseña un flujo simplificado para contingencias reales, pero exige el registro del ticket y la revisión formal del CAB en un plazo máximo de 24 a 48 horas tras el incidente.

💡 **Condiciona la aprobación al plan de reversión probado:** No apruebes ninguna solicitud de cambio que no incluya los pasos exactos, tiempos estimados y mecanismos de respaldo necesarios para regresar al estado previo ante un fallo.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política y el Procedimiento de Gestión de Cambios de TI. Durante la auditoría, seleccionará una muestra aleatoria de cambios ejecutados en los últimos meses (normales, estándar y de emergencia) y revisará en la herramienta de gestión de servicios (Jira, ServiceNow, GLPI) que cada solicitud cuente con su análisis de impacto, actas de pruebas en ambientes de homologación, plan de rollback, aprobación formal previa a la ventana de mantenimiento y registro de cierre exitoso; además, contrastará las bitácoras del sistema con los tickets para asegurarse de que no se realizaron modificaciones no autorizadas en producción.



Cláusula 8: Controles Tecnológicos

Control 8.33 Información de prueba

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

- **El Control:** La información de prueba debe ser adecuadamente seleccionada, protegida y gestionada.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en asegurar que los datos utilizados en actividades de desarrollo, aseguramiento de calidad (QA) y pruebas de sistemas no expongan información confidencial, secretos comerciales ni datos personales. Los puntos clave resumidos son:
 - Preferencia por Datos Sintéticos:** La regla general es evitar el uso de datos reales de producción y optar por generar datos ficticios o sintéticos que emulen la estructura y volumen necesarios.
 - Técnicas de Protección para Datos Reales:** Si resulta estrictamente indispensable utilizar una copia de datos de producción para pruebas complejas, se deben aplicar técnicas irreversibles de enmascaramiento, seudonimización o anonimización (en concordancia con el control 8.11).
 - Autorización Formal y Control de Acceso:** El uso de copias de datos reales en entornos de prueba requiere una justificación técnica documentada, aprobación explícita del propietario de los datos y control de acceso restringido al personal estrictamente necesario.
 - Eliminación y Limpieza Posterior:** Los datos de prueba derivados de entornos reales deben eliminarse de forma segura tan pronto concluyan las actividades de validación para evitar su permanencia indebida en servidores de desarrollo.
 - Registro de Auditoría:** Mantener bitácoras detalladas sobre la extracción, transferencia, uso y borrado de cualquier conjunto de datos derivado de producción.



Cláusula 8: Controles Tecnológicos

Control 8.33 Información de prueba

- **Otra Información:** La norma resalta que el uso descuidado de datos reales de clientes en entornos de testing representa una de las causas más frecuentes de violaciones de privacidad y sanciones bajo marcos regulatorios como el RGPD (GDPR) o leyes locales de protección de datos personales. Los entornos de prueba suelen tener controles perimetrales y de acceso más laxos que producción, convirtiéndolos en un blanco fácil para atacantes o filtraciones internas.

💡 **Utiliza generadores automáticos de datos ficticios:** Integra bibliotecas de generación sintética (como Faker o Mockaroo) en tus suites de pruebas unitarias para crear nombres, correos y tarjetas de crédito simuladas sin tocar bases productivas.

💡 **Aplica ofuscación antes de transferir datos fuera de producción:** Si es inevitable usar una muestra real, ejecuta los scripts de enmascaramiento y anonimización dentro del entorno productivo antes de exportar el volcado a los ambientes de QA.

💡 **Programa la destrucción automática de ambientes de prueba:** Configura procesos automáticos que eliminen bases de datos y contenedores de prueba al finalizar los ciclos de certificación de cambios para no acumular información residual.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará la Política de Protección de Datos de Prueba y el procedimiento para el aprovisionamiento de datos en ambientes no productivos. Durante la revisión, inspeccionará bases de datos en los entornos de desarrollo y control de calidad (QA); comprobará que no existan datos personales reales (nombres, identificaciones, tarjetas bancarias o teléfonos) sin enmascarar, y en caso de que se hayan utilizado datos de producción, exigirá la solicitud formal de justificación, la aprobación del dueño de la información y la evidencia de su destrucción posterior.



Cláusula 8: Controles Tecnológicos

Control 8.34 Protección de los sistemas de información durante las pruebas de auditoría

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

- **El Control:** Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de sistemas operacionales deben planificarse y acordarse entre el evaluador y la dirección adecuada.
- **Resumen de las Directrices de Implementación:** La guía de implementación se enfoca en regular cualquier actividad de evaluación técnica (auditorías de TI, escaneos de vulnerabilidades, pruebas de penetración o revisiones de configuración) sobre sistemas de producción para evitar caídas de servicio, degradación del rendimiento o corrupción de datos. Los puntos clave resumidos son:
 - Planificación y Alcance Formal:** Definir y acordar previamente el alcance exacto, los sistemas objetivo, las herramientas a utilizar y los horarios de ejecución de las pruebas.
 - Autorización de la Dirección:** Toda prueba técnica invasiva o de auditoría debe contar con la aprobación formal de los custodios del sistema y de la gerencia responsable.
 - Acceso de Solo Lectura:** El acceso otorgado a auditores y herramientas de evaluación debe limitarse estrictamente a permisos de solo lectura, salvo en pruebas específicas de penetración previamente delimitadas.
 - Monitoreo y Planes de Contingencia:** Supervisar activamente el comportamiento de los sistemas durante la ejecución de las pruebas y disponer de un canal de comunicación directo para detener la actividad si se detecta inestabilidad.
 - Custodia de Resultados:** Proteger los reportes y evidencias generadas durante la auditoría, ya que contienen detalles sobre vulnerabilidades críticas que podrían ser explotadas si se filtran.



Cláusula 8: Controles Tecnológicos

Control 8.34 Protección de los sistemas de información durante las pruebas de auditoría

- **Otra Información:** La norma resalta que cuando las pruebas involucren escaneos automatizados de vulnerabilidades o ethical hacking sobre infraestructura en la nube (AWS, Azure, GCP), se deben revisar previamente las políticas del proveedor cloud para evitar bloqueos por falsas alertas de ataque. Asimismo, si se realizan pruebas en sistemas industriales (OT/SCADA) o de soporte vital, el riesgo operacional es aún mayor, por lo que se recomienda priorizar entornos de laboratorio o réplicas antes de tocar producción.

💡 **Establece Reglas de Compromiso (Rules of Engagement - RoE):** Firma siempre un documento que delimite direcciones IP objetivo, ventanas de tiempo autorizadas, tipos de ataques prohibidos (como DoS destructivo) y contactos de emergencia antes de cualquier evaluación.

💡 **Ejecuta escaneos invasivos fuera del horario pico:** Programa los análisis automáticos de vulnerabilidades y pruebas de carga durante ventanas de bajo tráfico o fines de semana para mitigar riesgos de lentitud hacia los usuarios finales.

💡 **Revoca accesos de auditoría inmediatamente al concluir:** No dejes cuentas de auditor o permisos temporales de lectura activos; inhabilita o elimina todas las credenciales creadas específicamente para la evaluación tan pronto termine la revisión.

💡 **El Enfoque del Auditor (Lo que te van a revisar):** El auditor solicitará el Procedimiento de Planificación y Control de Pruebas de Auditoría y Aseguramiento Técnico. Durante la revisión, pedirá evidencia de las últimas evaluaciones realizadas (como auditorías internas de TI, escaneos de vulnerabilidades o reportes de pentesting); comprobará la existencia de acuerdos de alcance firmados, autorizaciones previas de la gerencia técnica, registros de monitoreo durante la ejecución de las pruebas y verificará que las cuentas temporales o herramientas utilizadas durante la evaluación hayan sido revocadas o desinstaladas al concluir el ejercicio.



Gracias por su atención



 www.valfraitconsulting.com

