Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO INTENSIVO

MÓDULO I

FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

Ing. Johnattan Sifuentes Rojas

MODULO I – FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

CONTENIDO MODULO I

1. Introducción a la Seguridad de la Información
2. La información como activo organizacional
3. Principios de la seguridad de la información: Confidencialidad, Integridad, Disponibilidad (CID)
4. Seguridad de la Información, Privacidad y Ciberseguridad.
5. Explorando la ISO 27001:2022 e ISO 27002:2022
6. La organización y el control de su información
7. Alcance y su importancia para el entorno de la organización.
8. Gestión de Incidentes de Seguridad de la Información
9. Gestión e Importancia de Controles en el Entorno de la Organización.

INTRODUCCION A LA SEGURIDAD DE LA INFORMACIÓN

INTRODUCCION A LA SEGURIDAD DE LA INFORMACIÓN

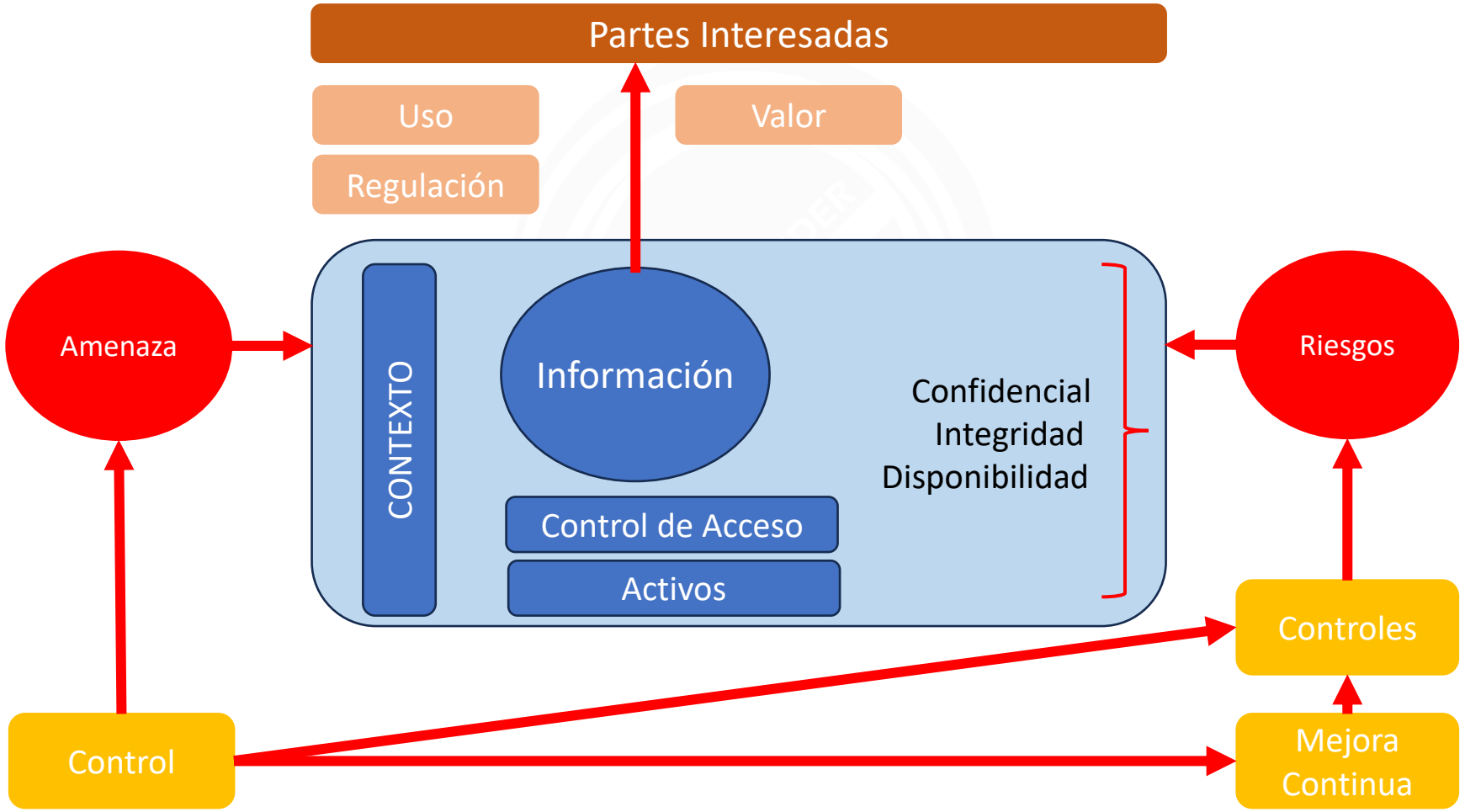
Definición de la Seguridad de la Información

La seguridad de la información involucra la **definición, implementación, mantenimiento y evaluación de un sistema de medidas coherentes que asegure la disponibilidad, integridad y confidencialidad (CID)** de la provisión de la información sea manual o computarizada.

Se enfoca en la **protección de la información y las características que le dan valor**, tales como confidencialidad, integridad y disponibilidad, e incluye la tecnología que alberga y transfiere esa información a través de una variedad de mecanismos de protección, como políticas, programas de capacitación y concientización y tecnología.

INTRODUCCION A LA SEGURIDAD DE LA INFORMACIÓN

SGSI en alto Nivel



PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

CID

Confidencialidad

- Evitar que personas no autorizadas puedan acceder a la información.
- Ejemplo:
  - Datos privados de las personas.
  - Propiedad intelectual de las empresas.
  - Seguridad nacional para países y gobiernos

Disponibilidad

- La información y los recursos relacionados estén disponibles para el personal autorizado.
- Es decir, se expresa como la cantidad de tiempo que los usuarios pueden usar un sistema, aplicación y datos.

Integridad

- Guardar la totalidad de la información, cuyo contenido debe permanecer inalterado a menos que sea modificado por personal autorizado.
- Es decir, tiene que ser precisa, validad y no haber tenido alteración.

SEGURIDAD DE LA INFORMACION, PRIVACIDAD Y CIBERSEGURIDAD

SEGURIDAD DE LA INFORMACION, PRIVACIDAD Y CIBERSEGURIDAD

Seguridad de la Información

¿Qué es la Seguridad de la Información?

La seguridad de la información es la práctica de proteger los datos y los sistemas de información de amenazas como el acceso no autorizado o las fugas de datos que provoquen la divulgación, alteración o destrucción de información sensible. La seguridad de la información incluye la aplicación de medidas críticas y procesos de control para garantizar la confidencialidad, integridad y disponibilidad de la información clave

SEGURIDAD DE LA INFORMACION, PRIVACIDAD Y CIBERSEGURIDAD

Privacidad

¿Qué es la Privacidad de la Información?

Llamada también Privacidad de los datos, es cuando una organización o individuo debe determinar que datos de un sistema de información puede ser compartidos con terceros (organizaciones o personas ajenas).
Para ello, debe considerar a quienes dará acceso y a quien no, y si cuenta con los mecanismos necesarios para prevenir cualquier acceso no autorizado a dicha información.

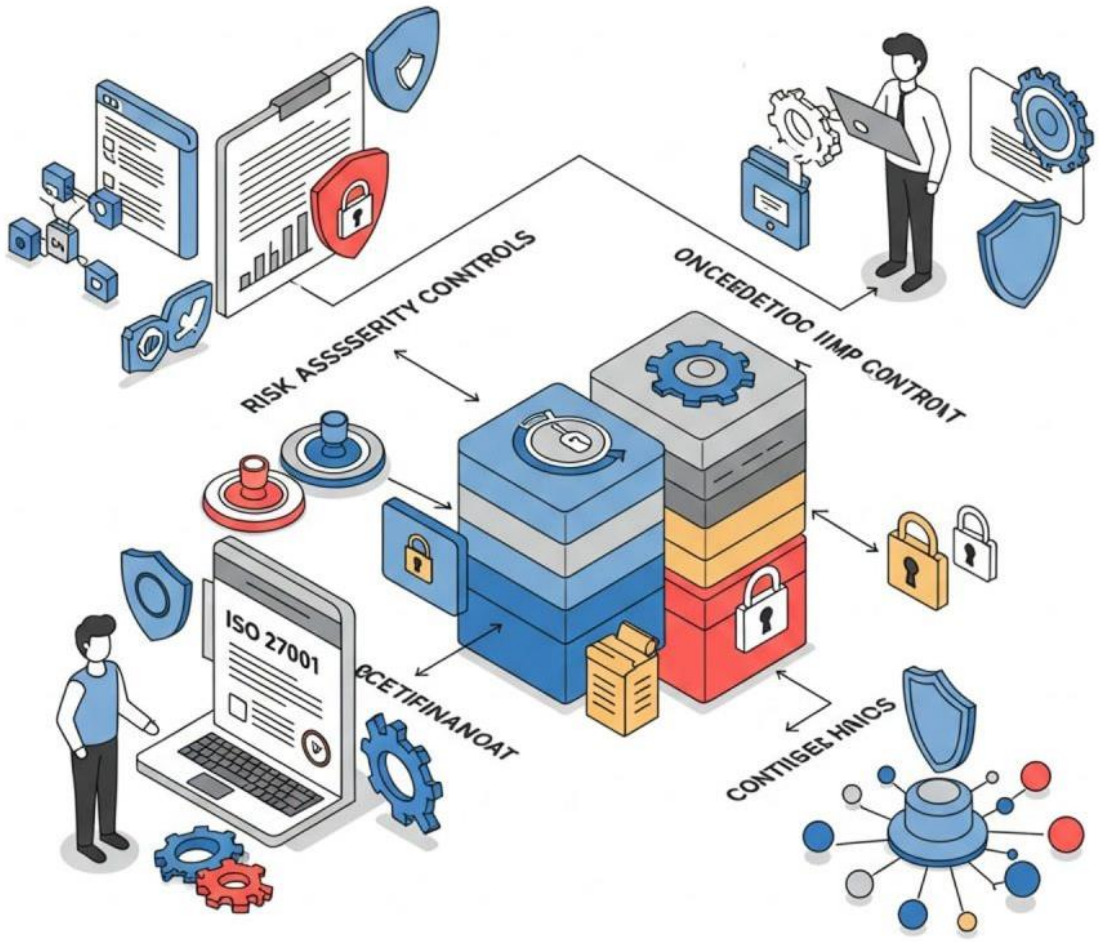
SEGURIDAD DE LA INFORMACION, PRIVACIDAD Y CIBERSEGURIDAD

Ciberseguridad

¿Qué es la Ciberseguridad?

Se define como un conjunto de medidas de protección de la información, a través del tratamiento de las amenazas que ponen en riesgo la información que es tratada por los sistemas de información que se encuentran interconectados, según ISACA

EXPLORANDO ISO 27001:2022 e ISO 27002:2022



¿Sabías que ?

El 60% de las empresas que sufren una brecha de seguridad significativa cierran en menos de seis meses?

La certificación ISO 27001 ayuda a prevenir estos riesgos y a fortalecer la resiliencia empresarial.

EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Familia ISO 27000 - Relaciones

Las normas de la seria 27000 nacen en 1995 con la BS 7799, redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan correctamente “ISO / IEC” porque son desarrolladas y mantenidas conjuntamente por dos organismos internaciones de normas : ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrónica Internacional), sin embargo, en el uso diario la parte “IEC” a menudo se descarta

Actualmente hay 71 normas publicados en la serie ISO 27000.

Estándar	Proposito	Caso de uso común	Capa de prueba
ISO / IEC 27001	Requisitos y certificación del SGSI	Certificación de línea base	Utilizado en más de 100,000 organizaciones
ISO / IEC 27002	Implementación de controles de seguridad.	Selección de control	Mapeo de controles
ISO / IEC 27005	Gestión de riesgos de seguridad de la información	Análisis de riesgos	Mapas de calor de riesgos, paneles de control
ISO / IEC 27701	Extensión de privacidad (adaptación al RGPD)	Integración de la privacidad de datos	Informes sobre el umbral de privacidad
ISO/IEC 27017/27018	Controles de la nube, información de identificación personal (PII) en nubes públicas	Implementaciones multiinquilino	Registros de cumplimiento de terceros

EXPLORANDO ISO 27001:2022 e ISO 27002:2022

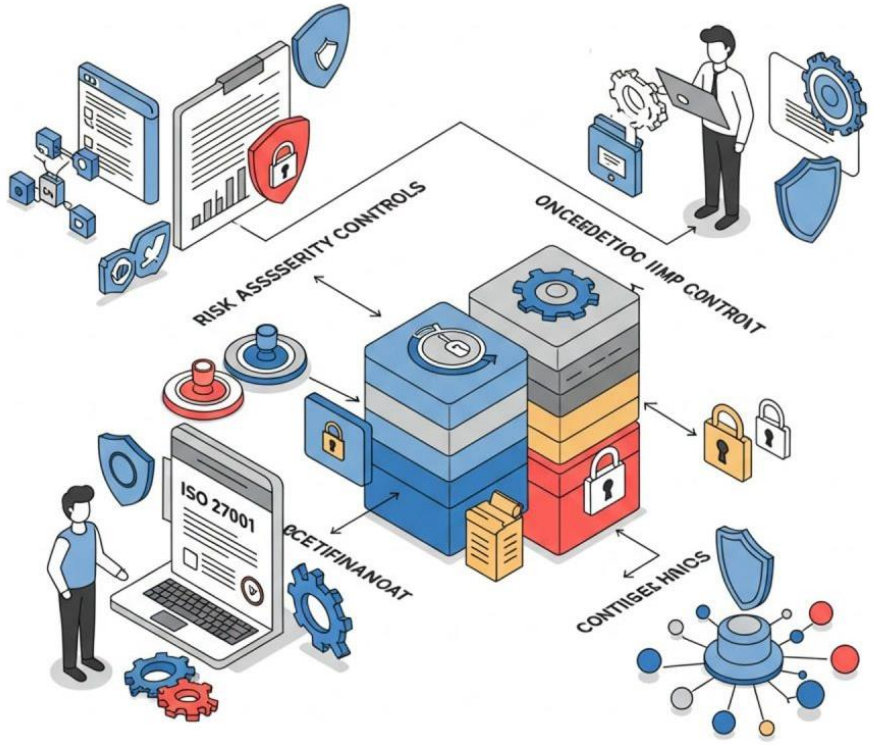
EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Norma ISO/IEC 27001:2022

Publicado 15 OCT 2005 y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene la capacidad de ser certificable en las empresas (SGSI).

Contiene un Anexo A, donde enumera en resumen los objetivos de control y controles.

Permite incorporarse al Sistemas de Gestión Integrado (SIG) para las normas internacionales como ISO 9001:2015, ISO 14001:2015, ISO 27001:2013, ISO 37001:2016 (por ejemplo)

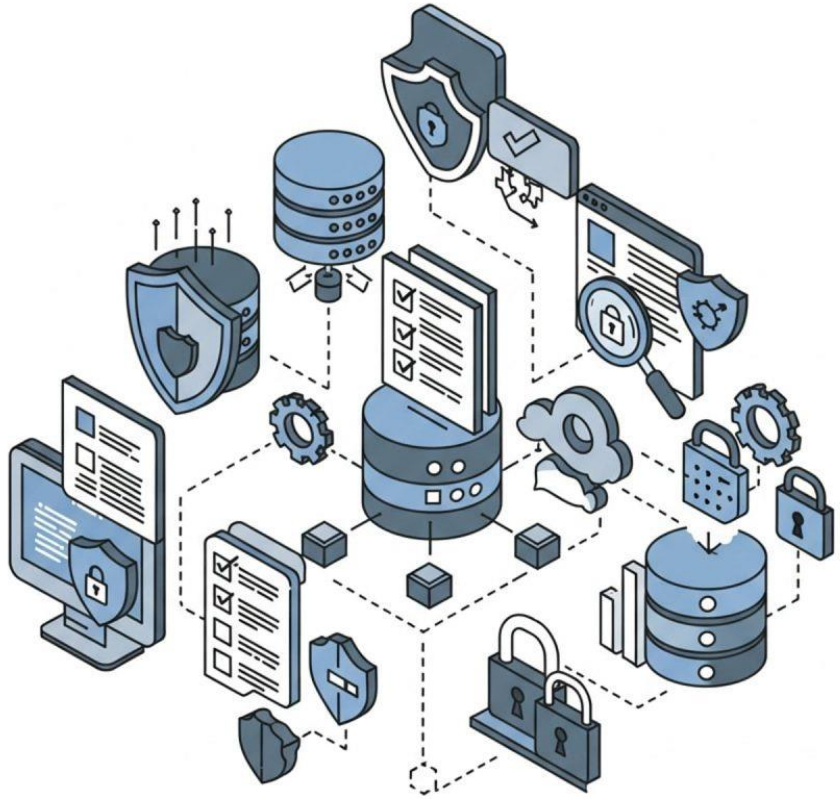


EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Objetivo de ISO/IEC 27001:2022

El objetivo principal de la norma ISO 27001 es ayudar **a las organizaciones a proteger los activos de la organización, garantizando su confidencialidad, integridad y disponibilidad y recudir riesgos e incidencias.**

Otro de los principales objetivos de la norma, es el **enfoque del sistema de gestión de manera alineada con la estrategia de negocios de la organización.**



EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Introducción a la Norma ISO/IEC 27001:2022

La norma ha sido diseñada para **“proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información”**

La norma “**puede ser utilizada por partes interesadas y externa para evaluar la capacidad dela organización para cumplir con sus propios requisitos de seguridad de la información”**

La norma también incluye **“requisitos para la evaluación y tratamiento de los riesgos en la seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sea aplicables a toda las organizaciones, sin importar su tipo, tamaño o naturaleza”**

EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Norma ISO/IEC 27002:2022

Cambio de nombre de “**Tecnología de la Información – Técnicas de Seguridad – código de practicas para controles de Seguridad de la información”** a **“Seguridad de la información, Ciberseguridad y Protección de la Privacidad – Controles de Seguridad de la Información”.**

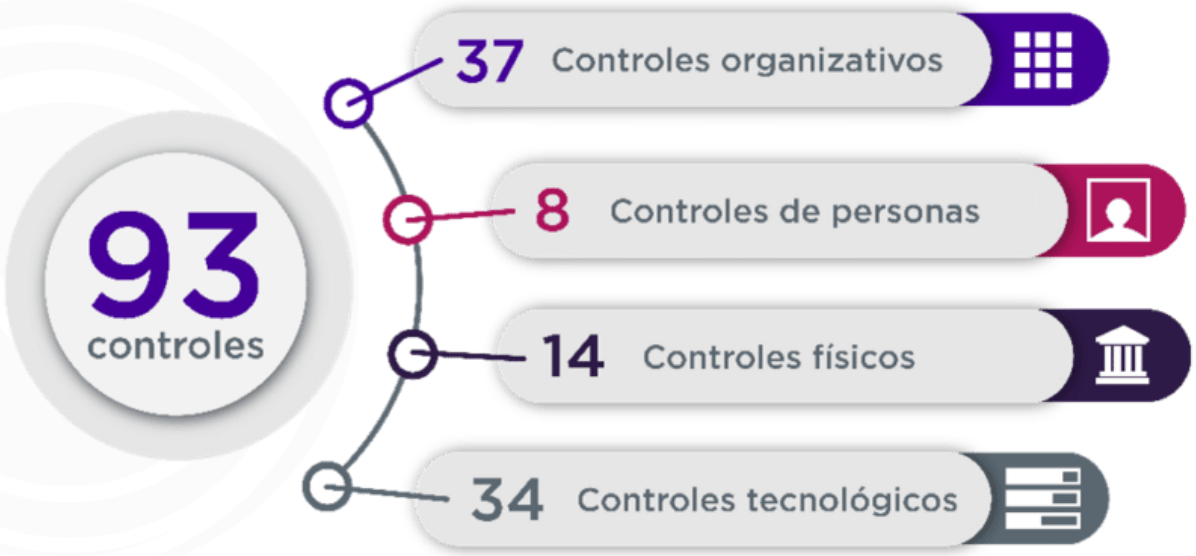
Se establecer 04 dominios para los controles: Organizacional, Personas, Físicos y Tecnológicos.

Se reducen el numero de controles de 114 a 93, producto de 58 controles se mantiene, la eliminación de 1 control y la fusión de 57 anteriores en 24 actuales, además de la inclusión de 11 nuevos controles.

EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Norma ISO/IEC 27002:2022

Se incluye nuevos términos:
Cadena de custodio
Información confidencial
Disrupción
Endpoint
Brechas de seguridad de la información
Personal, usuario
Información de identificación personal (PII)
PII principal, Procesador de PII
Evaluación del impacto de la privacidad
Punto objetivo de recuperación (RPO)
Tiempo objetivo de recuperación (RTO)
Regla
Información sensitiva
Política especifica

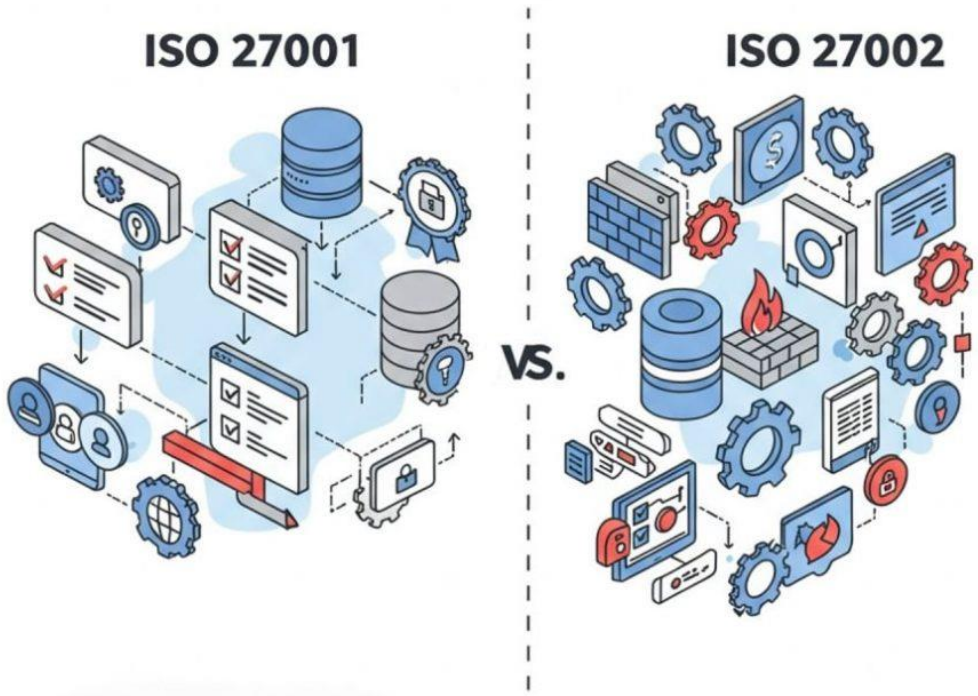


Permite integrar de manera mas clara, lo referente a ciberseguridad, privacidad de datos, gestión de indicades, gestión de la continuidad de negocio y gestión de la evidencia electrónica

EXPLORANDO ISO 27001:2022 e ISO 27002:2022

Diferencia entre ISO 27001 e ISO 27001

La ISO 27002 explica los controles de forma extensa, en contraste con el anexo A de la ISO 27001 que solo define una oración a cada uno (ambos usan la misma denominación).
No es posible obtener la certificación ISO 27002 porque no es una norma de gestión, solo es posible la certificación en ISO 27001 (tanto a nivel de personas como de organizaciones).
Se usa la ISO 27001 para crear y definir la estructura de la seguridad de la información en la organización (SGSI), se una la ISO 27002 para implementar y ejecutar controles.



LA ORGANIZACIÓN Y EL CONTROL DE SU INFORMACION

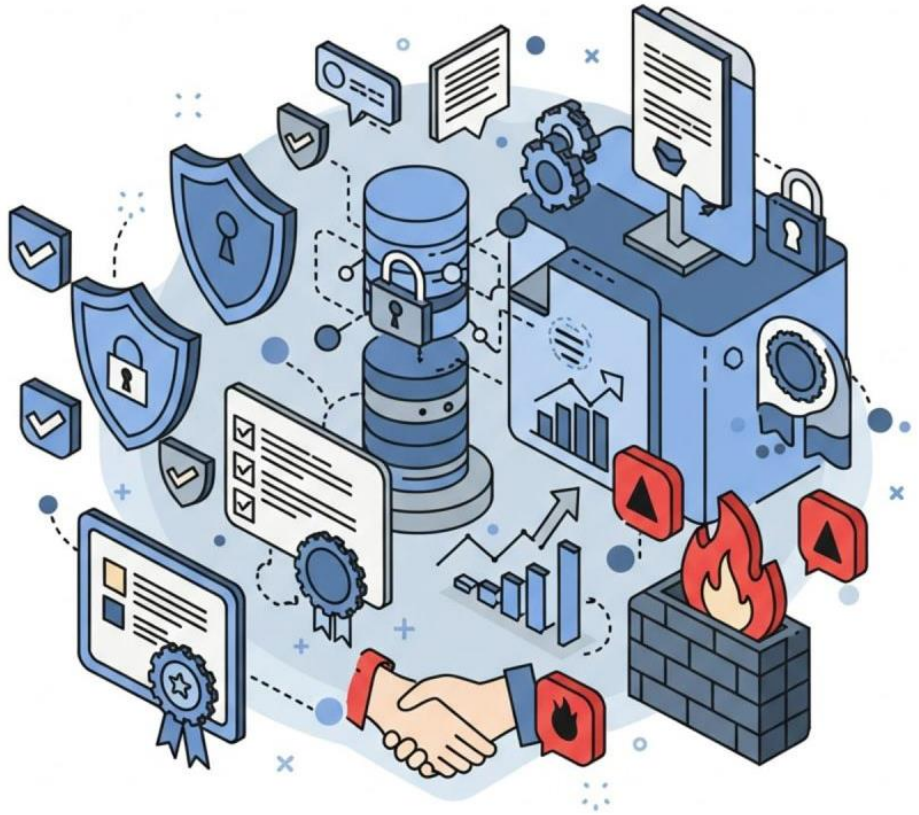
LA ORGANIZACIÓN Y EL CONTROL DE SU INFORMACION

Comprensión de la Organización y su contexto

Se trata del punto de partida para desarrollar el SGSI y consiste en determinar o identificar los “problemas” internos y externos a los que se enfrenta la organización.
Explicando de otra forma, el contexto organizacional consiste en considerar las expectativas y necesidades de todas las partes interesadas.

La forma y las áreas especificas de prioridad dependerán del contexto en el que opere su organización.
Se incluyen dos niveles:

- ✓ Interno: Aspectos sobre los que la organización tiene control
- ✓ Externo: Aspecto sobre los que la organización no tiene control directo.



LA ORGANIZACIÓN Y EL CONTROL DE SU INFORMACION

Comprensión de la Organización y su contexto

Una parte interesada es cualquier persona que sea, pueda ser o se considere afectada por una acción u omisión de su organización.

Sus partes interesadas serán claras atreves del proceso de llevar a cabo un análisis exhaustivo de los problemas internos y externo. Probablemente incluirán accionistas, propietarios, reguladores, clientes, empleados y competidores, y pueden extenderse al publico en general y al medio ambiente, dependiendo de la naturaleza de su negocio.

No tiene que tratar de comprender o satisfacer todos sus caprichos, pero si tiene que determinar cuales de sus necesidades y expectativas son relevantes para su SGSI.

LA ORGANIZACIÓN Y EL CONTROL DE SU INFORMACION

Comprensión de la Organización y su contexto

Alcance del SGSI:
Debe documentar el alcance del SGSI, los cuales suelen describir:

- Los limites del sitio físico o sitios incluidos (o no incluidos)
- Los limites de las redes físicas y lógicas incluidas (o no incluidas)
- Los grupos de empleados internos y externo incluidos (o no incluidos)
- Los procesos, actividades o servicios internos y externos incluidos (o no incluidos)
- Interfaces clave en los limites del alcance.

ALCANCE Y SU IMPORTANCIA PARA EL ENTORNO DE LA ORGANIZACON

ALCANCE Y SU IMPORTANCIA PARA EL ENTORNO DE LA ORGANIZACON

Importancia del liderazgo y compromiso

El liderazgo significa una participación activa en la dirección del SGSI, promover su implementación y garantizar la disponibilidad de recursos apropiados. Esto incluye:

- Asegurar que los objetivos del SGSI sean claros y estén alineados con la estrategia general.
- Claridad sobre las responsabilidades
- Que el pensamiento basado en el riesgo este en el corazón de toda la toma de decisiones
- Comunicación clara de esta información a todas las personas dentro del alcance del SGSI.

ALCANCE Y SU IMPORTANCIA PARA EL ENTORNO DE LA ORGANIZACON

Política de la Seguridad de la Información

La alta dirección de la organización debe liderar la implantación del SGSI demostrando su compromiso con el SGSI:

- Asegurándose de que las políticas y objetivos del SGSI están establecidos he integrados con los procesos de la organización.
- Asegurándose que el SGSI cuenta con los recursos necesarios para lograr los resultandos esperados.
- Asegurándose de que las personas entiendan cuan importante es realmente la seguridad de la información.
- Aliente a los gerentes a demostrar su liderazgo y compromiso con la seguridad de la información dentro de sus propias áreas

ALCANCE Y SU IMPORTANCIA PARA EL ENTORNO DE LA ORGANIZACON

Roles y responsabilidades

Para que las actividades de seguridad de la información formen parte de las actividades cotidianas para el personal de la organización, las responsabilidades que tiene deben definirse y comunicarse claramente.

Aunque NO hay algún requisito en la norma respecto al nombramiento de una representante de seguridad de la información, puede ser útil para algunas organizaciones designar a uno para dirigir un equipo de seguridad de la información que coordine la capacitación, el control de los controles y la presentación de informes sobre el desempeño del SGSI a la gerencia.

Sin embardo, para llevar a cabo su función de manera efectiva, lo ideal seria que fuese miembro de la gerencia y con conocimiento de la gestión de seguridad de la información.

ALCANCE Y SU IMPORTANCIA PARA EL ENTORNO DE LA ORGANIZACON

Roles y responsabilidades

Los roles de la seguridad de la información pueden variar en el titulo que se les entrega, pero no se alejan de lo siguiente:

- **Chief Information Security Office (CISO)**, es el nivel de gestión mas alto y desarrolla la estrategia general para el negocio completo.
- **Information Security Office (ISO),** desarrolla la política de una unidad de negocio basada en la política de la compañía y asegura que esta sea observada y ejecutada.
- **Information Security Manager (ISM),** desarrolla la política de seguridad de la información dentro de la organización de TI y asegura que sea revisada.

Adicionalmente a estos roles que son orientados específicamente a la seguridad de la información, una organización puede tener un Oficial de Política de Seguridad de la Información o un Oficial de Protección de Datos.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

¿Qué es un plan de respuesta a incidentes?

Un plan de respuesta a incidentes es un conjunto de pasos y directrices diseñados para detectar, responder y recuperarse de incidentes de seguridad como:

Filtraciones de datos | **Ciberataques** | **Malware** | **Errores humanos**

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Incidentes y Desastres en Seguridad de la Información

Es importante que toda organización, considere un plan de gestión de incidentes para:

- Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

- Definir roles y responsabilidades dentro de la organización como base para evaluar los riesgos y permitir mantener la operación, la continuidad y la disponibilidad de los servicios.

- Definir procedimiento de reporte y escalamiento (respuesta) formales ante un incidente de seguridad de la información.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Incidentes y Desastres en Seguridad de la Información

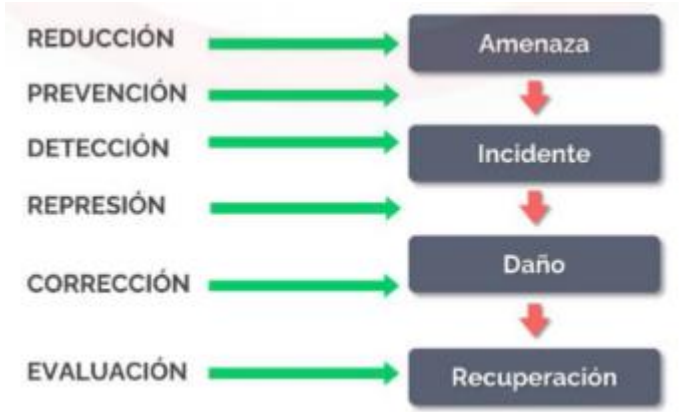
Incidente de Seguridad de la información:
Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.
Ejemplo: Un hacker logra ingresar a la red de la compañía

Desastre de Seguridad de la Información:
Uno o mas incidentes que amenazan la continuidad de Seguridad de la Información en la empresa.
Ejemplo: Uno o mas hackers eliminan activos de información críticos, causando una perdida importante a la empresa.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Ciclo de Incidente

Organización y enfoque



ISO 27035

Cubre los procesos para gestionar eventos, incidentes y vulnerabilidades de SI

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

NIST Cyber Security Framework PowerPoint Template

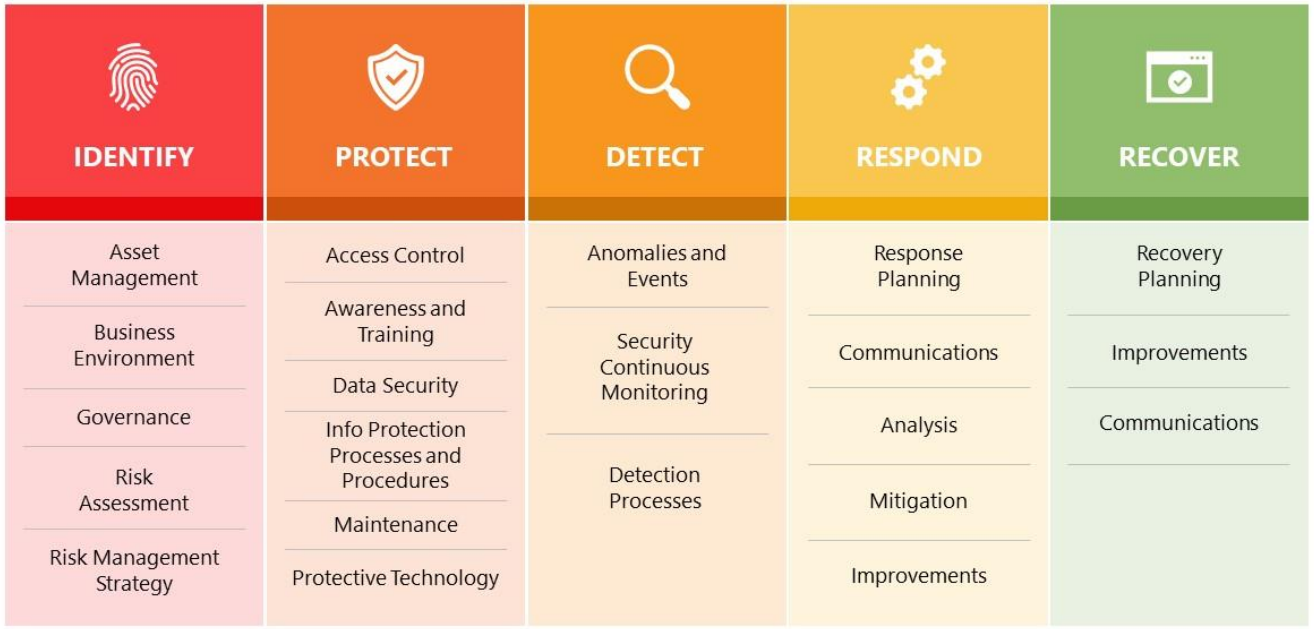


Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

GESTION E IMPORTANCIA DE CONTROLES EN EL ENTORNO DE LA ORGANIZACION

¿Qué es un control de ciberseguridad?

GESTION E IMPORTANCIA DE CONTROLES EN EL ENTORNO DE LA ORGANIZACION

Controles de Organización

ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad
Proporcionar un conjunto de referencia de controles genéricos de seguridad de la información, incluyendo una guía de implementación.

Permite abordar de forma mas clara temas de ciberseguridad y privacidad de la información, y que las organizaciones tengan la posibilidad de desarrollar sus propias directrices, basadas en la gestión de riesgos de seguridad de la información.

Priorizar el enfoque y protección de los activos de información basándose en la residencia, protección, defensa y gestión.

GESTION E IMPORTANCIA DE CONTROLES EN EL ENTORNO DE LA ORGANIZACION

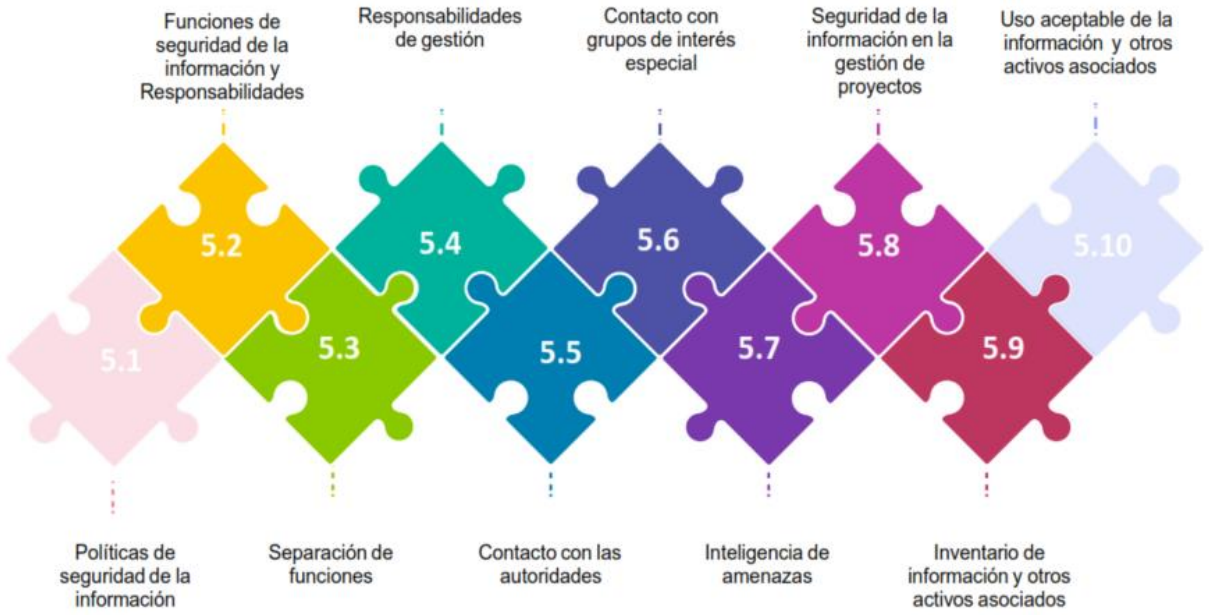
Controles de Organización

Características

Los controles organizacionales están estrechamente relacionados con los controles técnicos.

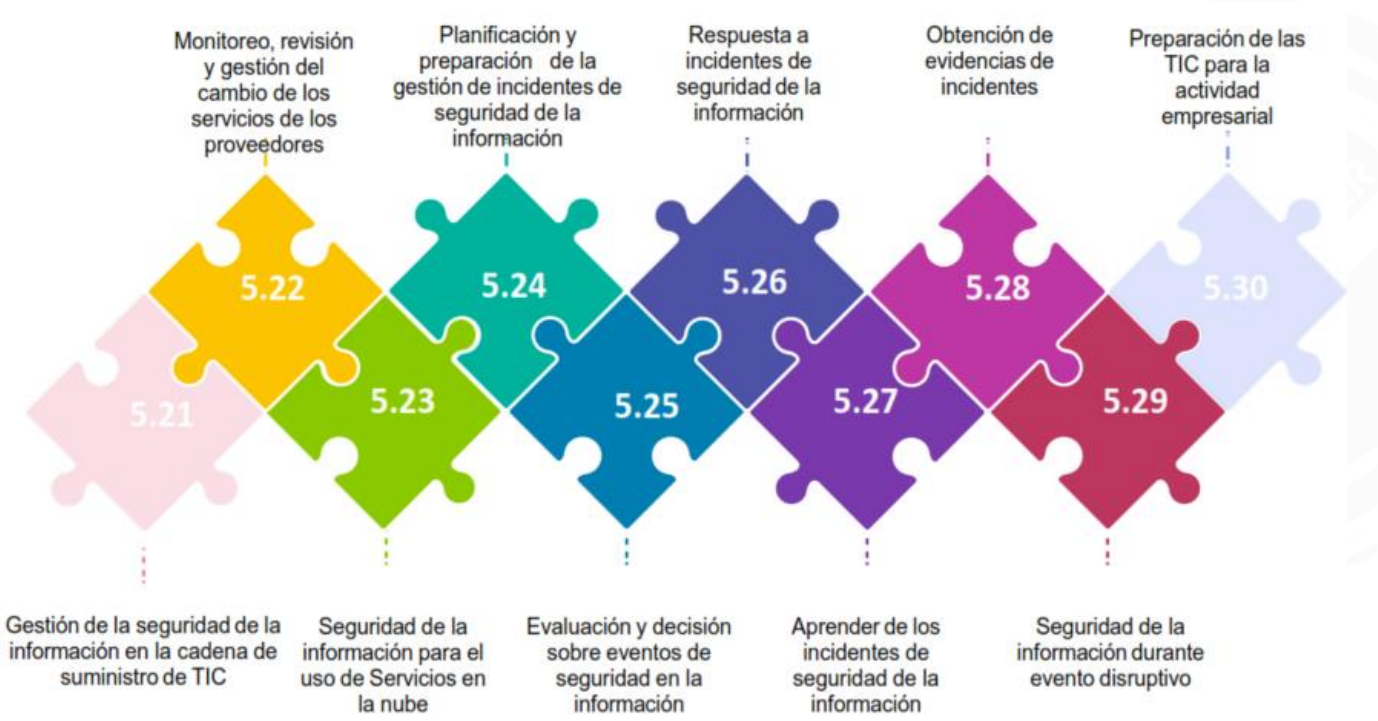
El ciclo PDCA (mejora continua) es una forma de implementar Seguridad de la Información en la organización, de como comercializarlos y lidiar con los desastres para estar preparados.

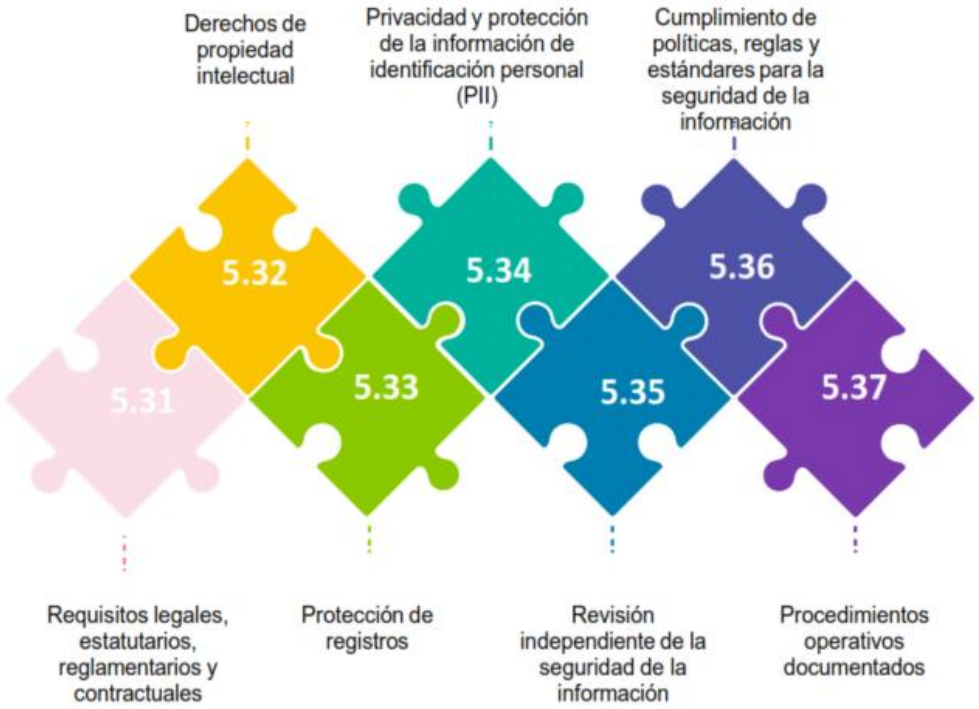
Los controles organizacionales están relacionados a los aspectos de comunicación, operación, procedimientos de prueba y la gestión de seguridad de la información



GESTION E IMPORTANCIA DE CONTROLES EN EL ENTORNO DE LA ORGANIZACION

Controles de Organización



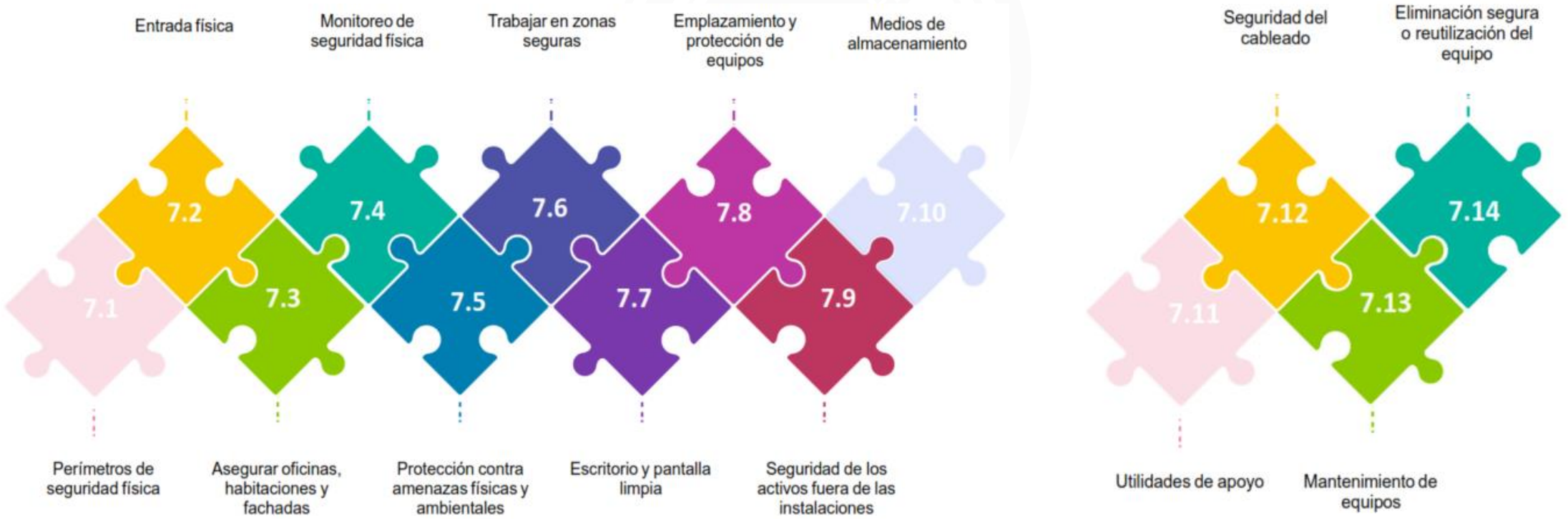


GESTION E IMPORTANCIA DE CONTROLES EN EL ENTORNO DE LA ORGANIZACION

Controles de Seguridad Física

Características

La seguridad física emplea una combinación de medidas organizativas, estructurales y electrónicas. Las medidas de Seguridad física necesitan ser planificadas y coordinadas de forma coherente. Las categorías principales son: Anillos de protección, alertas, alarmas contra incendios, planes de emergencia, áreas alrededor del edificio, el espacio de trabajo y el objeto (activo).



GESTION E IMPORTANCIA DE CONTROLES EN EL ENTORNO DE LA ORGANIZACION

¿Por qué es fundamental fortalecer los controles en la organización?

- ☑ Asegurar el cumplimiento regulatorio y normativo
- ☑ Proteger la información, los datos y la propiedad intelectual
- ☑ Resguardar los activos y documentos críticos del negocio
- ☑ Prevenir el uso indebido de los recursos de TI
- ☑ Garantizar el cumplimiento de políticas y estándares de seguridad
- ☑ Monitorear la efectividad de los controles y facilitar auditorías

¿Qué actos están asociados a este cumplimiento?

- ☑ Obtener y gestionar el consentimiento válido para el tratamiento de datos personales
- ☑ Proteger la confidencialidad, integridad y disponibilidad de la información
- ☑ Aplicar controles de acceso a sistemas y datos
- ☑ Clasificar, resguardar y eliminar adecuadamente la información
- ☑ Reportar oportunamente incidentes o brechas de seguridad
- ☑ Cumplir con políticas, procedimientos y estándares de seguridad
- ☑ Facilitar procesos de monitoreo y auditoría
- ☑ Capacitar y concientizar al personal en seguridad de la información

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad