GRUPODATCO

FOCUS
Una empresa de GRUPO DATCO

Creamos futuro

PROYECTO: IMPLEMENTACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Diciembre 2024

Información: Datos significativos.

Activo: Cualquier bien que tiene valor para la organización.

SEGURIDAD DE LA INFORMACIÓN

La SI es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones : confidencialidad, disponibilidad e integridad de la misma.

Asegura que la información sea accesible sólo para quienes tienen la autorización respectiva.

Garantiza la exactitud y completitud de la información.

Certifica que la información se encuentre disponible cuando sea requerida.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI

Un activo de información es cualquier recurso que tiene valor para una organización y que es esencial para la operación

- ✓ Políticas
- ✓ Procesos
- ✓ Controles
- ✓ Gestión Riesgos
- ✓ Roles
- ✓ Gobierno

Un SGSI permite la protección de los activos de información física y digital mediante la implementación de políticas, procesos y controles con el objetivo de que estos cuenten con atributos de confidencialidad, integridad y disponibilidad.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

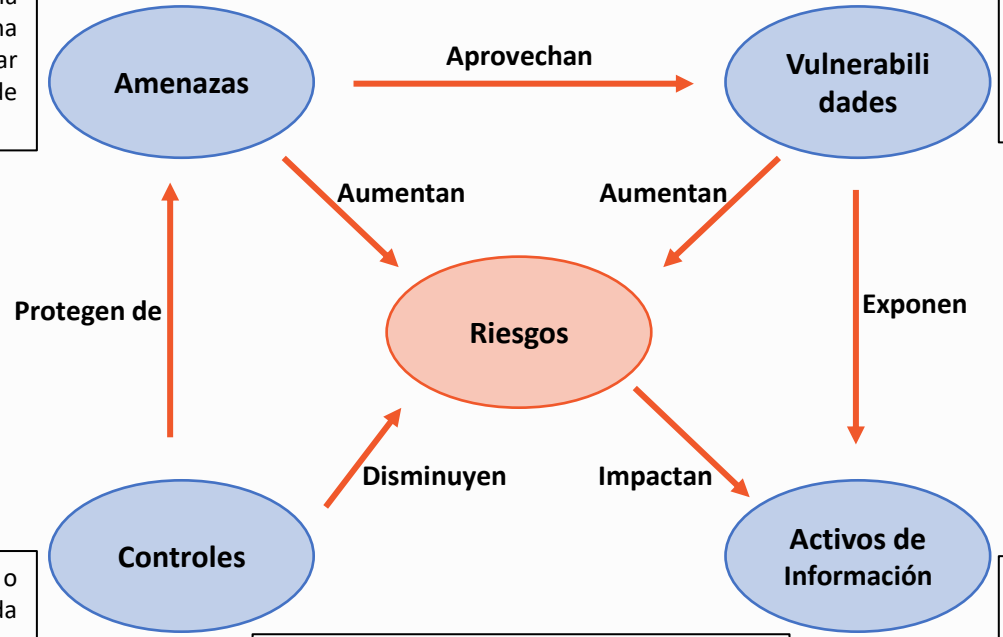
Componente	Seguridad de la Información (SI)	Sistema de Gestión de Seguridad de la Información (SGSI)
Definición	Es la práctica de proteger la **confidencialidad, integridad y disponibilidad** de los activos de información.	Es un conjunto estructurado de políticas, procesos y controles basado en la norma ISO/IEC 27001.
Alcance	Se enfoca en la implementación de medidas técnicas, organizativas y físicas para proteger información.	Es más amplio: incluye la **planificación, implementación, monitoreo y mejora continua** del sistema.
Normatividad	Generalmente, no está formalmente regulada, aunque sigue buenas prácticas (ej., usar cifrado, políticas de acceso).	Está basada en normas internacionales como la **ISO/IEC 27001:2022**.
Enfoque	Reaccionario, enfocado en solucionar problemas inmediatos relacionados con la seguridad.	Proactivo, busca prevenir riesgos a través de análisis, controles y mejora continua.
Documentación	Usualmente limitada a procedimientos operativos.	Requiere documentación formal, como políticas, análisis de riesgos, objetivos y procedimientos.
Monitoreo y Mejora	No siempre incluye un proceso estructurado de monitoreo y mejora.	Incluye procesos sistemáticos de evaluación (auditorías internas, revisiones de dirección, etc.).
Certificación	No se certifica como un sistema formal.	Puede certificarse para demostrar conformidad con la ISO/IEC 27001.

La Seguridad de la Información es un componente técnico/operativo que protege los activos de información. Un SGSI, en cambio, es un enfoque integral y gestionado que asegura que las medidas de seguridad sean consistentes, documentadas y mejoradas continuamente. Ambos son importantes, pero el SGSI proporciona un marco organizado y auditable para gestionar la seguridad de la información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Ejemplo	Seguridad de la Información (SI)	Sistema de Gestión de Seguridad de la Información (SGSI)
Control de Acceso	Configurar contraseñas robustas en sistemas y restringir el acceso por roles.	Diseñar y documentar un procedimiento formal para la gestión de acceso basado en ISO 27001.
Gestión de Vulnerabilidades	Actualizar software para corregir fallas de seguridad conocidas.	Establecer un proceso documentado de gestión de vulnerabilidades y análisis periódico de riesgos.
Protección contra Malware	Instalar antivirus en equipos de trabajo.	Documentar políticas y procedimientos de protección, además de monitorear continuamente la eficacia.
Gestión de Incidentes	Responder de forma inmediata a un ataque de phishing detectado.	Implementar un procedimiento formal de respuesta a incidentes, con roles y responsabilidades definidos.
Gestión de Riesgos	Usar medidas ad-hoc según la situación.	Realizar análisis de riesgos periódicos y planificar controles adecuados para mitigarlos.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



Es un evento o acción potencial que podría explotar una vulnerabilidad y causar daño a un activo de información.

Es una debilidad o falla en los sistemas, procesos o controles que puede ser aprovechada por una amenaza.

Medida técnica, organizativa o administrativa implementada para reducir, mitigar o eliminar riesgos asociados a la seguridad de la información.

Es la **probabilidad** de que una amenaza explote una vulnerabilidad de un activo de información, causando un **impacto** negativo en la confidencialidad, integridad o disponibilidad de dicho activo.

Recurso que tiene valor para una organización y que es esencial para la operación.

No.	Activo de Información	Vulnerabilidad	Amenaza	Riesgo	Probabilidad	Impacto	Control (es)	Responsable
1	Cuentas críticas	Uso de contraseñas débiles en cuentas críticas	Ataque de fuerza bruta o robo de contraseñas	Acceso no autorizado a información confidencial	Alta	Crítico	Implementar autenticación multifactor Establecer políticas de contraseñas seguras	Responsable de TI
2	Aplicaciones críticas	Falta de parches de seguridad en aplicaciones críticas	Explotación de vulnerabilidades conocidas	Interrupción de servicios o fuga de datos	Alta	Muy Alto	Aplicar gestión de parches y actualizaciones regulares	Administrador de sistemas
3	Sistemas de autenticación	Empleados que reutilizan contraseñas en múltiples sistemas	Robo de credenciales	Compromiso de múltiples sistemas debido al uso de las mismas credenciales	Alta	Crítico	Implementar políticas de contraseñas únicas Capacitación en seguridad para empleados	Responsable de Recursos Humanos y TI
4	Sistema de gestión de accesos	Políticas insuficientes para la gestión de permisos en el acceso a datos confidenciales	Asignación de privilegios no autorizada	Acceso indebido a datos confidenciales	Media	Muy Alto	Establecer control de acceso basado en roles Auditorías regulares de permisos	Oficial de Seguridad de la Información

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ISO 27001

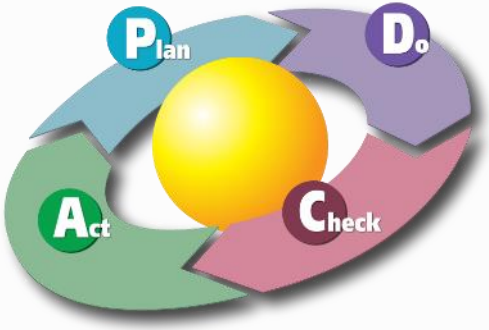
SGSI

- Establecer
- Implementar
- Mantener
- Mejorar

✓ Qué?
X Cómo?

ISO 27002

CICLO DE DEMING



NORMA ISO 27001: 2022

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Cumplimiento Normativo

↓

PCM 09/23: Resolución 003-2023-PCM/SGTD

↓

Mejorar Market Share

FOCUS
Una empresa de GRUPO DATCO

Gracias

Somos Grupo Datco, creamos futuro

grupodatco.com

company/grupodatco grupodatco grupodatco

GRUPODATCO