



Cyber

Protect

Data

Threat

Security

Attack

Firewall

Malware

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Garay Diaz, Juan Francisco - 17-5165-2009

Rosales Velásquez, José David - 17-0671-2022

Meza Mejía, Kevin José - 17-3278-2021

Internet 2 - Vicente Zarceno

UTEC



Mayo 2025





SGSI ¿QUÉ ES? ¿CÓMO IMPLEMENTARLO?

🔍 <http://www.securityforum.org/> 🔗



INTRODUCCIÓN

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, normas y herramientas organizadas de forma sistemática, cuyo objetivo es gestionar y proteger la información de una organización, garantizando su confidencialidad, integridad y disponibilidad. El SGSI se basa generalmente en normas internacionales como la ISO/IEC 27001 quien (a su vez) hace uso del conocido "**Ciclo de Deming**" Plan-Do-Check-Act (PDCA o PHVA) que significa "Planificar-Hacer-Verificar-Actuar"



Ciclo de Deming

INTRODUCCIÓN

SOBRE NORMA ISO 27001



La ISO 27001 es una norma que establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). Su fin es proteger los activos de información de una organización, asegurando su confidencialidad, integridad y disponibilidad, mediante la gestión de riesgos y la implementación de controles de seguridad.

Más info: <https://www.normaISO27001.es/>



INTRODUCCIÓN

SOBRE NORMA ISO 27002

Si bien la ISO 27001 es la norma principal para certificar un Sistema de Gestión de la Seguridad de la Información (SGSI), existe un marco de trabajo complementario que es fundamental para su implementación: la ISO 27002.

En resumen, si la ISO 27001 define "qué" debe tener un SGSI, la ISO 27002 te dice "cómo" implementarlo a través de controles específicos y detallados. Es la guía por excelencia para construir y mantener un SGSI robusto.





Cyber

Protect

Data

Threat

Security

Attack

Firewall

Malware

ALCANCES

SGSI

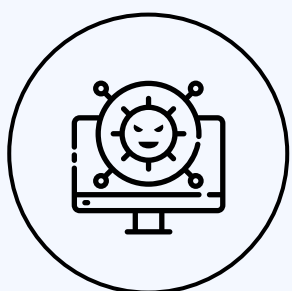


UTEC





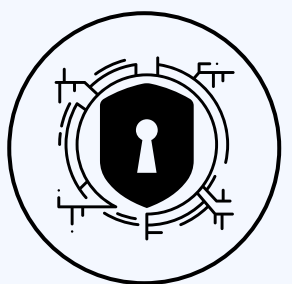
DEFINICIÓN DE ALCANCES



El SGSI permite a las organizaciones identificar los riesgos que amenazan su información, aplicar controles adecuados para mitigarlos y establecer procesos de mejora continua en materia de seguridad. Su enfoque está basado en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), lo que ayuda a mantener una gestión activa y adaptable frente a los cambios internos o externos.



Este sistema abarca la protección de datos digitales, físicos y en tránsito, así como la formación del personal, gestión de accesos, monitoreo de amenazas y respuestas ante incidentes de seguridad. Al implementar un SGSI, las organizaciones no solo fortalecen su postura ante ciberataques o pérdidas de información, sino que también cumplen con normativas legales, aumentan la confianza de sus clientes y protegen su reputación.



Un SGSI eficaz no es solo una herramienta tecnológica, sino un modelo de gestión integral que involucra a todos los niveles de la organización para crear una cultura de seguridad.





ALCANCES



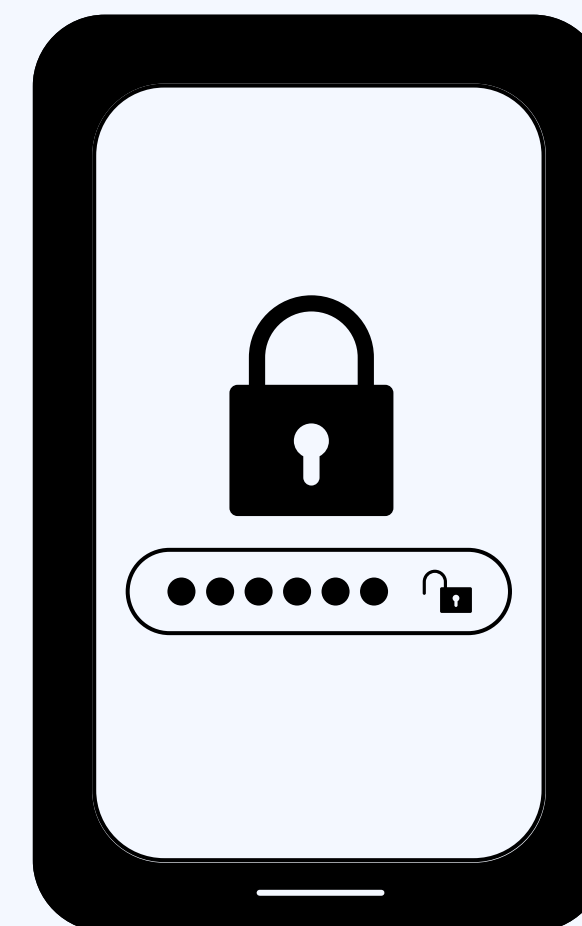
El alcance del SGSI define los límites y la aplicabilidad del sistema dentro de una organización. Establecerlo correctamente es esencial para enfocar los esfuerzos en los activos críticos y en los procesos que realmente requieren protección. A continuación, se describen los principales alcances que debe considerar un SGSI:

1. Alcance organizacional:

El SGSI puede aplicarse a toda la organización o solamente a una parte específica, como un departamento, sede, unidad de negocio o área de TI. Esta decisión debe basarse en los objetivos estratégicos, los riesgos identificados y los recursos disponibles.

2. Alcance geográfico:

Incluye las ubicaciones físicas donde se aplica el SGSI. Puede tratarse de una única oficina o de múltiples sedes distribuidas geográficamente, considerando las diferencias legales, normativas y operativas entre ellas.





ALCANCES



3. Alcance de los activos de información:

Se deben identificar los activos de información cubiertos por el SGSI, tales como:

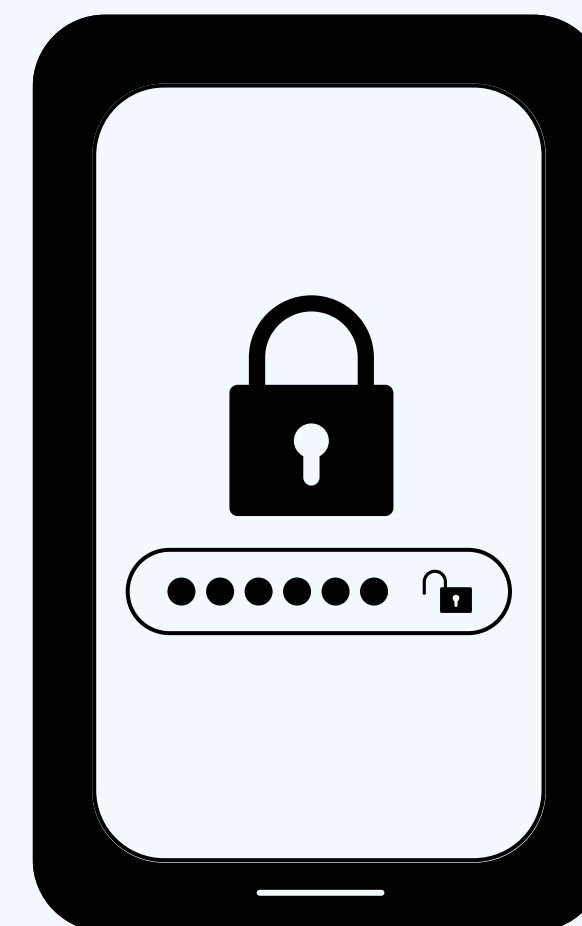
- Documentos físicos y digitales
- Bases de datos
- Sistemas y aplicaciones
- Infraestructura tecnológica (servidores, redes, dispositivos)
- Información confidencial de clientes, empleados y socios

4. Alcance de los procesos:

Especifica los procesos organizativos incluidos en el SGSI. Por ejemplo, puede abarcar procesos como gestión de usuarios, desarrollo de software, atención al cliente, compras, recursos humanos, entre otros.

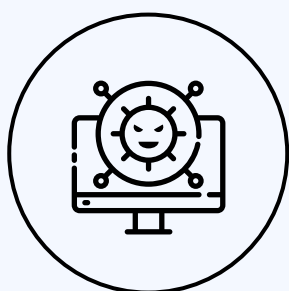
5. Alcance en cuanto a partes interesadas:

El SGSI también debe considerar a todas las partes interesadas relevantes, como empleados, proveedores, clientes, socios estratégicos y autoridades regulatorias. Se deben establecer mecanismos para garantizar que todas estas partes cumplan con las políticas de seguridad establecidas.





CÓMO IMPLEMENTAR

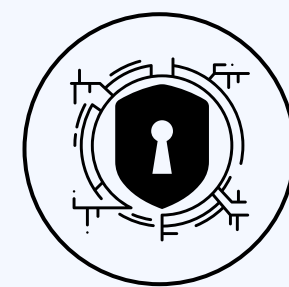


Fases de Implementación de un SGSI (ISO 27002)

Implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la ISO 27002 sigue el ciclo de mejora continua PDCA (Planificar-Hacer-Verificar-Actuar):

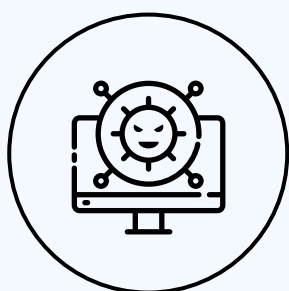
1. Planificar (Plan)

- Compromiso de la Alta Dirección: La dirección asegura los recursos y el apoyo para el SGSI.
- Definir el Contexto y Alcance: Se establecen los límites y las partes interesadas del SGSI.
- Establecer Política de Seguridad: Se define la declaración formal del compromiso con la seguridad.
- Identificación y Evaluación de Riesgos: Se identifican, analizan y priorizan las amenazas y vulnerabilidades de la información.
- Tratamiento de Riesgos: Se decide cómo gestionar los riesgos identificados, implementando o aceptando controles.
- Declaración de Aplicabilidad (SoA): Se documenta qué controles de ISO 27002 son aplicables y cómo se implementan.





CÓMO IMPLEMENTAR



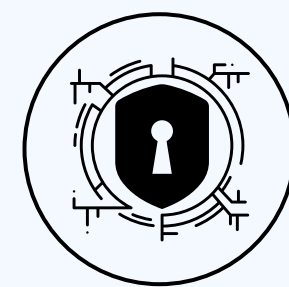
2. Hacer (Do)

- Implementación de Controles y Procedimientos: Se ponen en práctica las medidas de seguridad y los procesos definidos.
- Formación y Concientización: Se capacita al personal sobre las políticas y sus responsabilidades de seguridad.
- Gestión de Incidentes: Se establece el proceso para responder, investigar y aprender de los eventos de seguridad.



3. Verificar (Check)

- Monitoreo y Medición: Se evalúa la efectividad de los controles y el rendimiento del SGSI.
- Auditorías Internas: Se realizan revisiones periódicas para verificar el cumplimiento y la eficacia del SGSI.
- Revisión por la Dirección: La alta dirección evalúa el rendimiento del SGSI y su adecuación continua.



4. Actuar (Act)

- Mejora Continua: Se implementan acciones correctivas y preventivas para optimizar el SGSI.



Desventajas



Desventaja

- ⚠️ Alta exposición a amenazas
- 📄 Pérdida de información valiosa
- 💰 Costos por incidentes de seguridad
- 🔍 Incumplimiento legal
- 👤 Pérdida de confianza del cliente
- 📊 Falta de control de riesgos
- ⊖ Dificultades para certificarse o participar en licitaciones
- 🚒 Mala gestión de incidentes

Riesgo o consecuencia

Mayor vulnerabilidad a hackeos, pérdida de datos o accesos no autorizados.

No existen políticas claras de respaldo o protección.

Ransomware, recuperación de datos, sanciones legales, demandas.

Sanciones por no cumplir normativas como ISO 27001, LOPD, RGPD, etc.

Una brecha de seguridad puede afectar gravemente la imagen empresarial.

Las amenazas no se identifican ni gestionan de forma proactiva.

Muchas empresas exigen estándares como ISO 27001 para trabajar juntas.

Sin planes ni procedimientos definidos para actuar ante incidentes.





La Implementación de un SGSI en „Chivo Wallet S.A. de C.V.





Cyber

Protect

Data

Threat

Security

Attack

Firewall

Malware

EJEMPLO DE IMPLEMENTACIÓN

Chivo Wallet SA



UTEC





EJEMPLO DE IMPLEMENTACIÓN

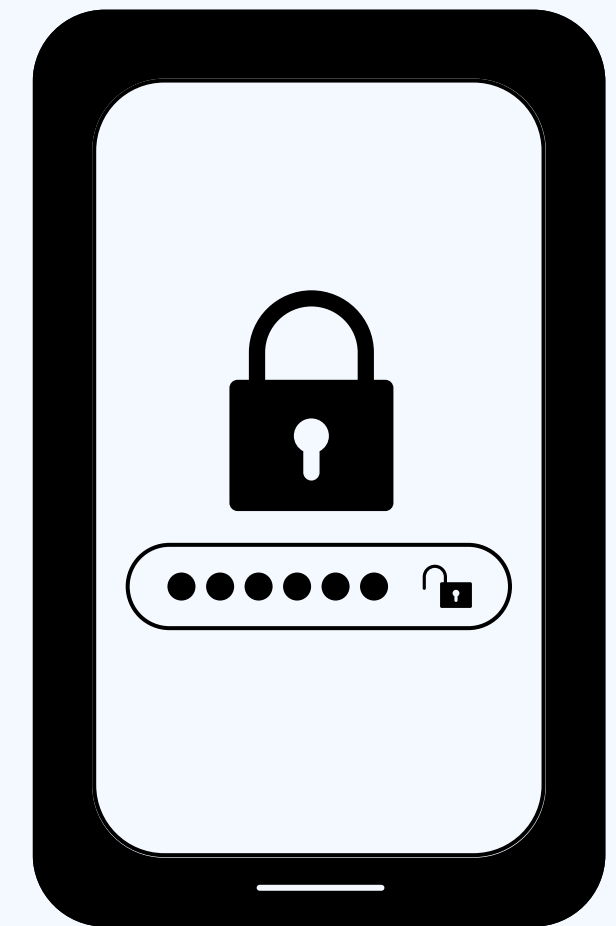


Chivo Wallet S.A. de C.V. decide implementar un SGSI basado en la norma ISO 27001/27002, siguiendo el ciclo PDCA:

Fases de Implementación:

1. Planificar (Plan):

- **Compromiso de la Alta Dirección:** El presidente de la empresa nombra un **Comité de Seguridad de la Información** y asigna un presupuesto.
- **Definir Contexto y Alcance:** Se analiza el entorno de Chivo Wallet y se decide que el SGSI cubrirá los procesos de desarrollo de software y la gestión de datos de clientes.
- **Política de Seguridad:** Se crea una política de alto nivel que establece los principios de seguridad de la información.
- **Análisis y Tratamiento de Riesgos:** Se identifican activos (código fuente, bases de datos de clientes), amenazas (ciberataques, errores humanos), vulnerabilidades (sistemas desactualizados) y se evalúan los riesgos. Se decide mitigar la mayoría con controles específicos.





EJEMPLO DE IMPLEMENTACIÓN



2. Hacer (Do):

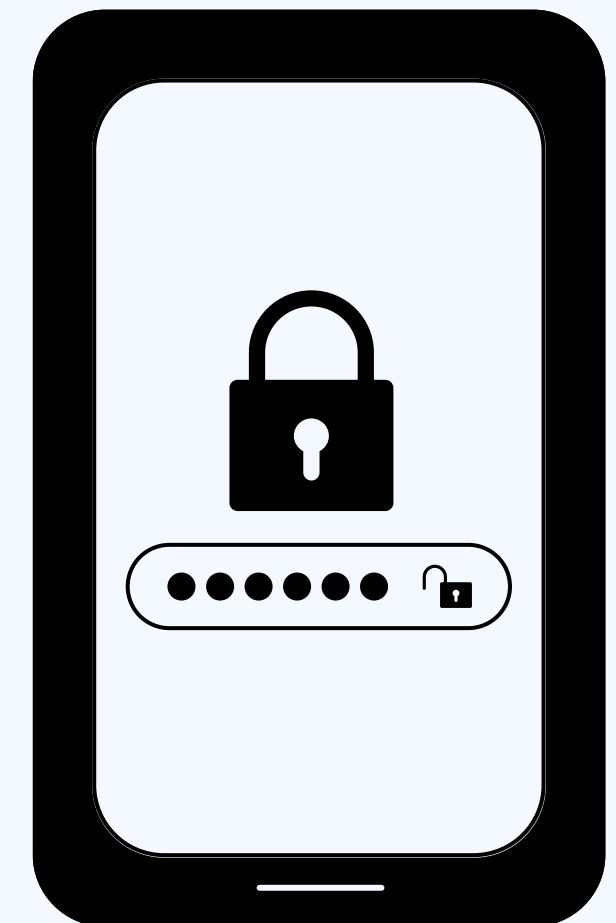
- **Implementación de Controles:** Se implementan controles como: políticas de contraseñas fuertes, doble factor de autenticación, cifrado de datos, copias de seguridad automatizadas, formación en ciberseguridad para empleados, control de acceso basado en roles, y procedimientos de desarrollo seguro.
- **Documentación:** Se desarrollan y documentan todos los procedimientos y registros necesarios para el SGSI.

3. Verificar (Check):

- **Monitoreo:** Se implementan herramientas para monitorear el tráfico de red, logs de sistemas y actividad de usuarios.
- **Auditorías Internas:** Un equipo interno, capacitado en ISO 27001, realiza auditorías periódicas para identificar brechas.
- **Revisión por la Dirección:** El Comité de Seguridad de la Información se reúne semestralmente para revisar el desempeño del SGSI y tomar decisiones estratégicas.

4. Actuar (Act):

- **Mejora Continua:** Se corrigen las no conformidades detectadas en las auditorías, se ajustan los controles según las nuevas amenazas y se optimiza el SGSI constantemente.

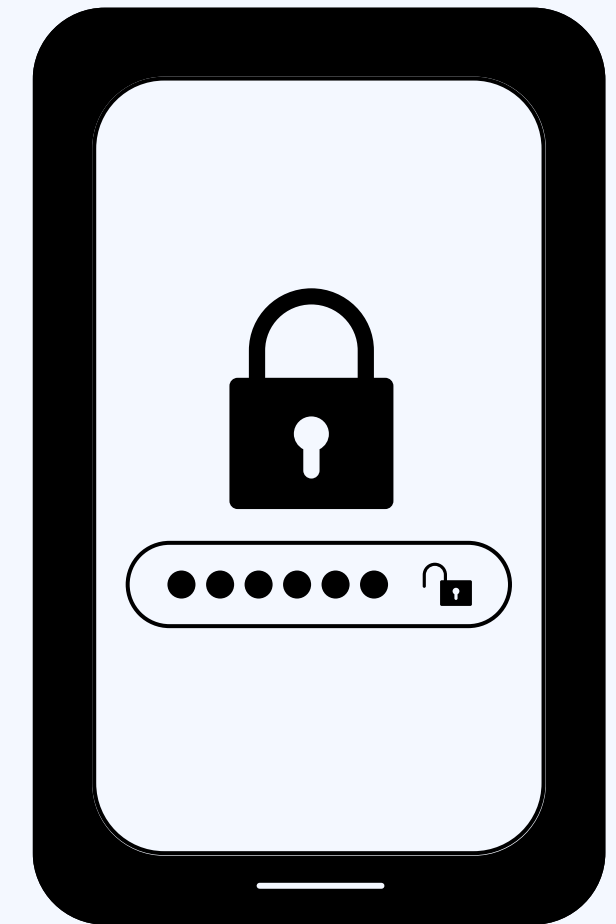




ROLES NECESARIOS



- **Comité de Seguridad de la Información:** Grupo de alto nivel (con la CEO, CTO, CISO, y un representante legal/RRHH) que supervisa la estrategia del SGSI y toma decisiones clave.
- **Oficial de Seguridad de la Información (CISO):** Rol dedicado, responsable de la implementación, mantenimiento y mejora del SGSI. En TechSolutions, el CTO asume este rol inicialmente y luego se contrata a un CISO.
- **Líderes de Proceso/Dueños de Activos:** Gerentes de área o individuos responsables de la seguridad de la información dentro de sus respectivos dominios (ej. Gerente de Desarrollo, Gerente de Operaciones de TI).
- **Equipo de Implementación del SGSI:** Personal técnico y administrativo que ayuda a desarrollar la documentación, implementar controles y gestionar los procesos diarios del SGSI.
- **Audidores Internos de SGSI:** Personal capacitado para realizar las auditorías internas del sistema.












Ventajas



Ventaja

Descripción

-  Protección de la información
-  Reducción de riesgos
-  Cumplimiento legal y normativo
-  Confianza de clientes y socios
-  Mejora continua
-  Auditorías más efectivas
-  Gestión de incidentes
-  Toma de decisiones informada
-  Protección en entornos híbridos/cloud

- Asegura la confidencialidad, integridad y disponibilidad de los datos.
- Identifica, analiza y controla los riesgos de seguridad.
- Facilita el cumplimiento de leyes como la Ley de Protección de Datos o requisitos contractuales.
- Mejora la reputación y credibilidad ante terceros.
- El ciclo PDCA permite adaptar los controles a nuevas amenazas.
- Permite realizar auditorías internas y externas con base sólida.
- Reduce el impacto de incidentes y permite una respuesta rápida y ordenada.
- Basada en análisis de riesgos y evaluación de controles.
- Aplicable a infraestructuras físicas y digitales.





Cyber

Protect

Data

Threat

Security

Attack

Firewall

Malware

RESULTADO DE LA IMPLEMENTACIÓN

SGSI



UTEC





RESULTADO DE LA IMPLEMENTACIÓN



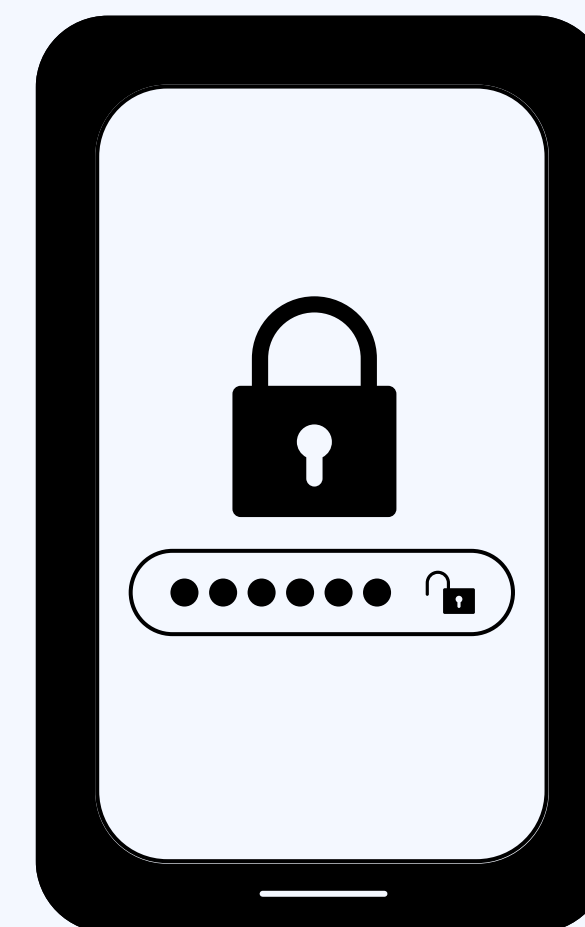
La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) trae consigo una serie de resultados positivos y tangibles que fortalecen la protección de los activos de información y mejoran la eficiencia organizacional. Estos resultados varían según el tamaño y el tipo de organización, pero entre los más relevantes se encuentran los siguientes:

1. Mayor protección de la información:

Uno de los principales resultados es la reducción significativa de riesgos relacionados con la pérdida, filtración o modificación no autorizada de la información. Los controles implementados permiten prevenir incidentes y responder eficazmente cuando ocurren.

2. Cumplimiento normativo y legal:

Un SGSI bien estructurado facilita el cumplimiento de normativas y leyes relacionadas con la seguridad y la protección de datos, como la ISO/IEC 27001, la Ley de Protección de Datos Personales o regulaciones sectoriales. Esto evita sanciones legales y mejora la relación con autoridades y clientes.





RESULTADO DE LA IMPLEMENTACIÓN



3. Mayor confianza de clientes y socios:

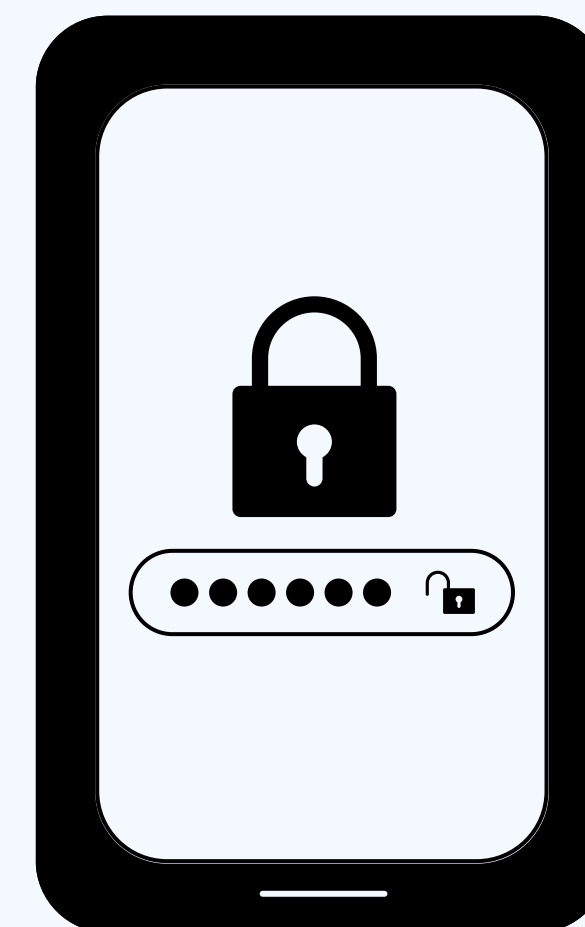
Las organizaciones que demuestran contar con un SGSI generan confianza y credibilidad ante sus clientes, proveedores y socios, ya que aseguran el manejo responsable de la información y la protección de datos sensibles.

4. Mejora en la gestión de riesgos:

La organización se vuelve más proactiva en la identificación, evaluación y mitigación de riesgos, lo que le permite tomar decisiones informadas y anticiparse a posibles amenazas.

5. Estandarización de procesos:

La implementación del SGSI lleva a la documentación y estandarización de procesos, lo que mejora la organización interna, reduce la improvisación y facilita la capacitación de nuevos empleados.





RESULTADO DE LA IMPLEMENTACIÓN



6. Fortalecimiento de la cultura de seguridad:

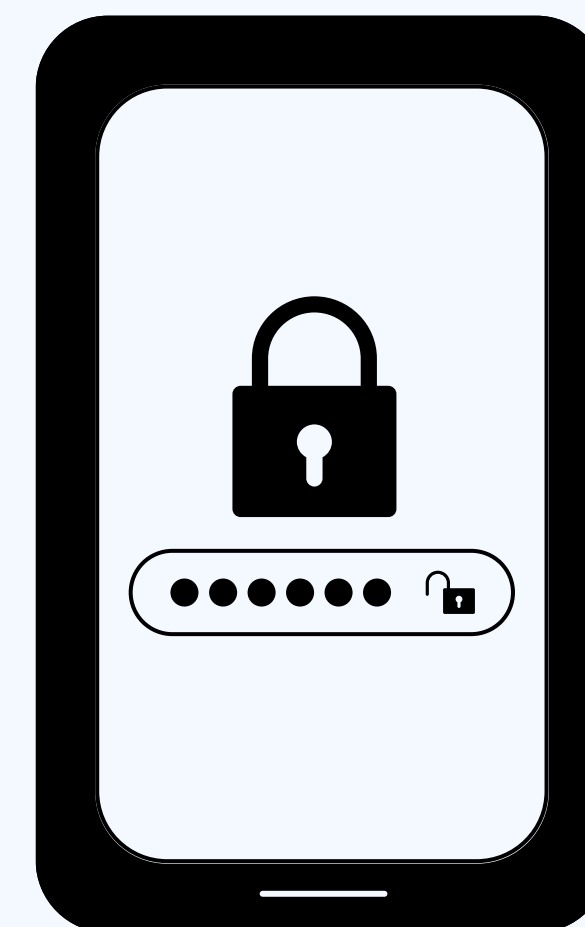
Con el tiempo, la organización desarrolla una cultura organizacional orientada a la seguridad, donde todos los empleados comprenden su rol en la protección de la información y adoptan buenas prácticas de forma natural.

7. Preparación ante incidentes:

Gracias al SGSI, la organización cuenta con protocolos de respuesta ante incidentes, lo que reduce el tiempo de reacción, minimiza impactos negativos y permite una recuperación más rápida.

8. Mejora continua:

El SGSI se basa en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar), lo que impulsa una mejora continua de las políticas, controles y procesos, adaptándose a los cambios tecnológicos y del entorno.





Cyber

Protect

Data

Threat

Security

Attack

Firewall

Malware

RECOMENDACIONES ADICIONALES

SGSI



UTEC





RECOMENDACIONES



4. Capacitación y concienciación del personal:

El factor humano suele ser el punto más débil en la seguridad de la información. Por ello, se recomienda capacitar periódicamente al personal en buenas prácticas, manejo de información confidencial y prevención de amenazas como el phishing o el uso inseguro de dispositivos.

5. Uso de controles tecnológicos adecuados:

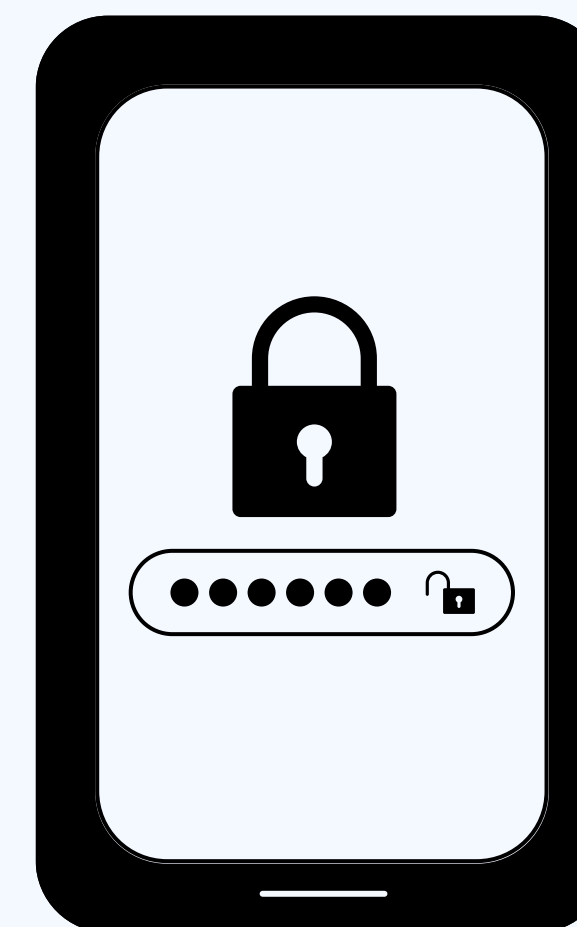
Implementar herramientas como firewalls, antivirus, sistemas de detección de intrusos, cifrado de datos y autenticación multifactor para proteger la infraestructura tecnológica.

6. Auditorías internas y mejora continua:

Realizar auditorías periódicas del SGSI permite identificar desviaciones, debilidades o incumplimientos. Con base en los hallazgos, se deben aplicar acciones correctivas para mejorar continuamente el sistema.

7. Cumplimiento normativo y legal:

Asegurarse de que el SGSI esté alineado con normativas y leyes aplicables en materia de protección de datos, como la ISO/IEC 27001, la Ley de Protección de Datos Personales, o marcos regulatorios locales.





Cyber

Protect

Data

Threat

Security

Attack

Firewall

Malware

MEJORES PRÁCTICAS

SGSI



UTEC





MEJORES PRÁCTICAS



La implementación y gestión exitosa de un SGSI requiere la adopción de mejores prácticas que ayuden a garantizar la seguridad de la información, el cumplimiento normativo y la mejora continua. A continuación, se detallan algunas de las mejores prácticas más recomendadas:

1. Aplicar el principio de "menor privilegio":

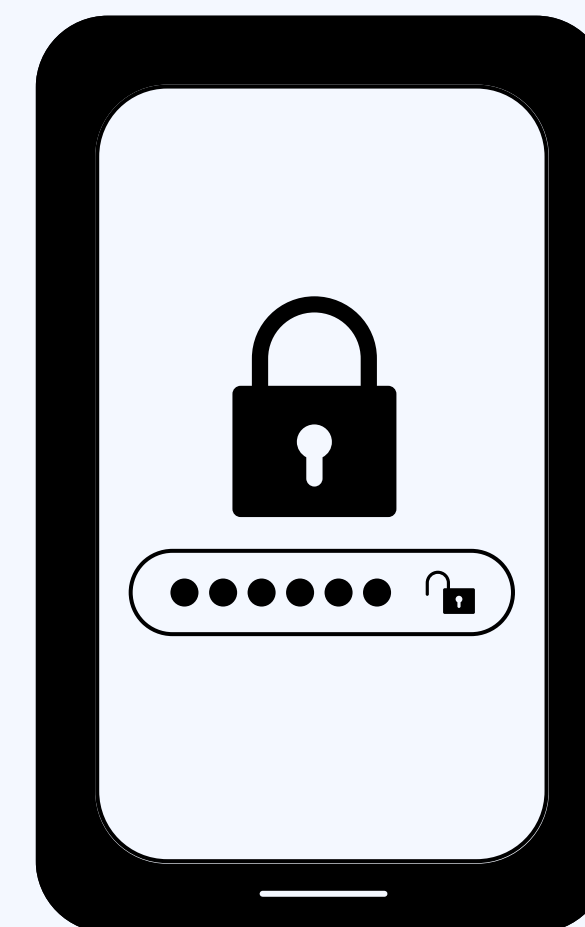
Los usuarios deben tener acceso solo a la información y recursos necesarios para realizar su trabajo. Esto reduce el riesgo de exposición o mal uso de datos sensibles.

2. Establecer una política de seguridad sólida:

Toda organización debe contar con una política de seguridad de la información formal, clara y alineada con los objetivos del negocio. Esta política debe ser comunicada a todo el personal y revisada periódicamente.

3. Gestionar adecuadamente los incidentes de seguridad:

Es crucial contar con un protocolo de gestión de incidentes que permita detectar, analizar, responder y recuperar ante cualquier incidente de seguridad (como accesos no autorizados, pérdidas de datos o ciberataques).





MEJORES PRÁCTICAS



4. Realizar análisis de riesgos periódicos:

El entorno tecnológico y los riesgos evolucionan constantemente. Por ello, es recomendable realizar evaluaciones de riesgos de forma continua para identificar nuevas amenazas y actualizar los controles de seguridad.

5. Mantener actualizado el inventario de activos:

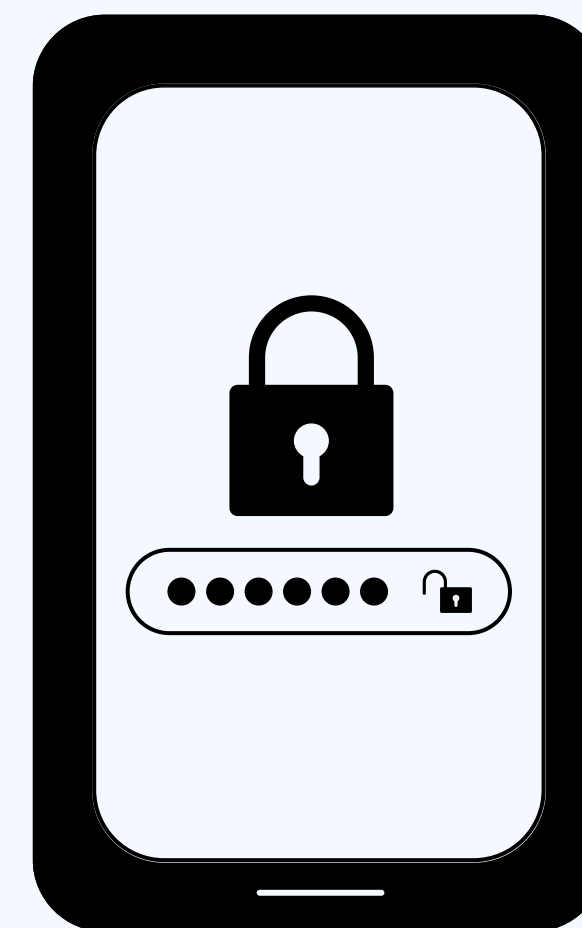
Tener un registro actualizado de los activos de información, su clasificación y su nivel de criticidad permite protegerlos de manera adecuada y priorizar los controles de seguridad.

6. Implementar controles de acceso fuertes:

Utilizar mecanismos de autenticación multifactor (MFA), contraseñas robustas y control de sesiones para asegurar que solo personal autorizado acceda a los sistemas e información.

7. Capacitar constantemente al personal:

El factor humano es esencial para el éxito del SGSI. Las organizaciones deben ofrecer capacitaciones regulares sobre buenas prácticas de seguridad, políticas internas y concienciación sobre amenazas comunes (como phishing o ingeniería social).





MEJORES PRÁCTICAS



8. Monitorear y auditar continuamente:

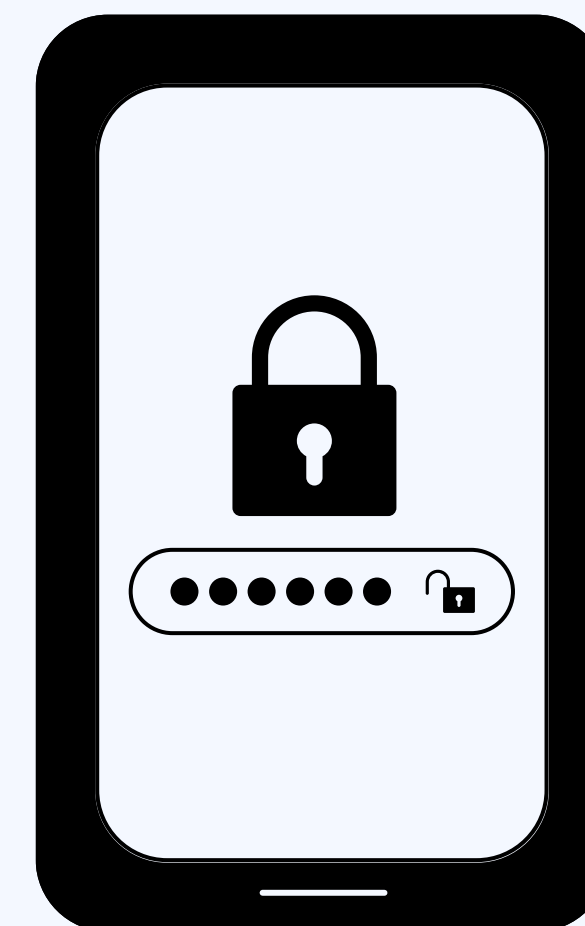
Utilizar herramientas de monitoreo continuo y realizar auditorías internas para detectar anomalías, evaluar la eficacia de los controles y asegurar el cumplimiento de las políticas del SGSI.

9. Gestionar adecuadamente los proveedores:

Asegurarse de que los proveedores externos también cumplan con los requisitos de seguridad de la organización, sobre todo si manejan información sensible o acceden a sistemas internos.

10. Fomentar la mejora continua:

El SGSI debe ser un sistema dinámico y en constante evolución. La revisión de indicadores, auditorías, retroalimentación del personal e innovaciones tecnológicas deben usarse como base para su mejora constante.





INGENIERIA DEL CAOS



Las pruebas tipo "**Chaos Monkey**" o, más ampliamente, la **Ingeniería del Caos**, son una excelente manera de probar la resiliencia y la efectividad del SGSI en un entorno real y adverso.

Estas pruebas, realizadas de forma controlada y planificada, ayudan a identificar puntos ciegos en los controles, deficiencias en los procedimientos de respuesta a incidentes y a fortalecer la resiliencia general del SGSI, superando la teoría de los documentos.

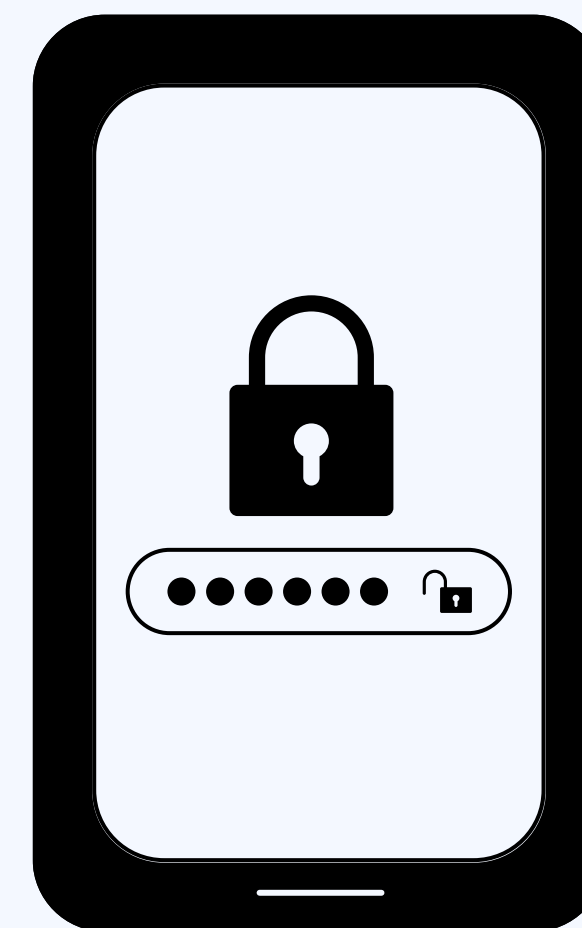




¿CÓMO APLICAR I.D.C. EN EL SGSI?



- **Interrupción simulada de servicios:** Desactivar repentinamente una base de datos secundaria o un servidor de respaldo para ver si los procedimientos de recuperación de desastres (parte del SGSI) funcionan como se espera.
- **Inyección de fallos en la red:** Simular problemas de conectividad para probar la redundancia de red y los mecanismos de conmutación por error.
- **Pruebas de denegación de servicio (DoS) controladas:** Evaluar la capacidad de los sistemas de protección (WAF, IPS/IDS) y los equipos de respuesta a incidentes para detectar y mitigar ataques.
- **Eliminación aleatoria de archivos o credenciales:** Probar la efectividad de las copias de seguridad, los controles de acceso y los sistemas de monitoreo de integridad.
- **Simulación de compromiso de credenciales:** Probar la capacidad de los sistemas de detección de intrusiones para identificar actividad sospechosa después de que se "compromete" una cuenta de prueba.



CONCLUSION



En un entorno cada vez más digital y expuesto a amenazas, la implementación de un SGSI se vuelve una necesidad estratégica para las organizaciones que desean proteger su información crítica, cumplir con normativas legales y fortalecer la confianza de sus clientes y socios. Este sistema permite gestionar de manera estructurada los riesgos asociados a la información, estableciendo controles, políticas y procesos que garantizan la confidencialidad, integridad y disponibilidad de los datos.

Además, el SGSI no solo es una herramienta técnica, sino un enfoque integral que involucra a toda la organización, fomenta una cultura de seguridad y permite la mejora continua. Su correcta implementación contribuye al crecimiento sostenible del negocio, reduce la exposición ante amenazas internas y externas, y posiciona a la organización como una entidad responsable y comprometida con la seguridad de la información.

