Sistema de Gestión de Seguridad de la Información (SGSI) - ISO 27001

Portada

Título: Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)
Autor: Luis Fernando Armenta Cruz
Fecha de Emisión: 31 de octubre 2024

Índice

- Referencias

---

1. Resumen Ejecutivo

El propósito del Sistema de Gestión de Seguridad de la Información (SGSI) es proteger los activos de información críticos de la organización, asegurando la confidencialidad, integridad y disponibilidad de los datos. Este sistema ha sido desarrollado en conformidad con el estándar ISO 27001, proporcionando un enfoque estructurado y sistemático para gestionar los riesgos de seguridad de la información.

El SGSI cubre todos los activos de información dentro de la organización, incluyendo servidores de aplicaciones, bases de datos, redes de comunicación y dispositivos de usuario, así como las áreas de recursos humanos, administración de TI y departamentos clave donde se maneja información sensible.

Los objetivos de este SGSI son garantizar que la información esté protegida de accesos no autorizados (confidencialidad), que la información sea precisa y completa (integridad), y que esté disponible cuando se necesite (disponibilidad).

El SGSI se basa en un enfoque integral de gestión de riesgos, que permite identificar y mitigar amenazas de manera efectiva. A través de evaluaciones de riesgo periódicas, se implementan controles específicos para reducir la exposición a vulnerabilidades y mejorar la postura de seguridad general de la organización.

El sistema incluye controles de acceso basados en roles, cifrado de datos en reposo y en tránsito, políticas de respaldo de información y actualizaciones automáticas para mantener todos los sistemas en las versiones más seguras. Además, se han implementado medidas de monitoreo continuo y procedimientos de respuesta a incidentes.

La organización está comprometida con la seguridad de la información y con la mejora continua de su SGSI. Este compromiso se refleja en las auditorías periódicas, el ajuste de políticas de acuerdo con las mejores prácticas y la capacitación continua del personal.

La implementación del SGSI aporta beneficios clave, incluyendo una mayor protección contra amenazas cibernéticas, cumplimiento con estándares internacionales, aumento de la confianza de los clientes en la organización y reducción de riesgos operativos.

---

2. Introducción al SGSI

2.1 Objetivo del SGSI

El objetivo principal de este SGSI es proteger la información crítica de la organización y sus activos de información, manteniendo la confidencialidad, integridad y disponibilidad de los datos. La implementación de este sistema se basa en los principios de la norma ISO 27001, buscando una protección estructurada y continua contra amenazas internas y externas.

2.2 Alcance y Contexto de la Organización

El SGSI se aplica a todos los activos de información de la empresa y cubre las áreas de tecnología, recursos humanos y administración de la red, protegiendo la infraestructura, datos de clientes y aplicaciones críticas. El contexto considera las amenazas cibernéticas actuales y los riesgos asociados con la exposición a internet**.**

2.3 Principios ISO 27001

- **Confidencialidad**: Asegurar que la información solo sea accesible por personas autorizadas.

- **Integridad**: Mantener la exactitud y completitud de la información y sus métodos de procesamiento.

- **Disponibilidad**: Garantizar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando lo requieran.

---

3. Análisis de Riesgos y Gestión de Vulnerabilidades

3.1 Identificación de Activos

Los activos de información incluyen:

- **Servidores de Aplicaciones**: Contienen bases de datos de clientes y sistemas críticos.
- **Red Local y VPN**: Protegen la comunicación interna y los accesos remotos.
- **Equipos de Usuarios**: PC y dispositivos utilizados por empleados para acceder a datos sensibles.

3.2 Evaluación de Amenazas y Vulnerabilidades

A partir del análisis del proyecto, se identificaron amenazas clave:

- **Ataques a puertos vulnerables**: Puertos como FTP (21), SSH (22), y HTTP (80) abiertos, que pueden ser explotados.

- **Exposición de datos sensibles**: Archivos y directorios en WordPress desactualizado que facilitan la explotación.
- **Vulnerabilidades de versiones obsoletas**: Paquetes como Apache, Exim, MySQL detectados en el escaneo inicial.

3.3 Análisis de Impacto y Probabilidad

La organización evalúa el impacto de cada vulnerabilidad mediante una clasificación de bajo, medio y alto impacto:

- **Impacto bajo**: Acceso no autorizado a datos de bajo riesgo.
- **Impacto medio**: Alteración de configuraciones críticas, con posible afectación a clientes.
- **Impacto alto**: Pérdida o robo de información crítica y posible escalación de privilegios.

3.4 Matriz de Riesgos y Tratamiento

Cada riesgo se categoriza en una matriz considerando la probabilidad e impacto:

- **Riesgo alto**: Vulnerabilidad en el puerto 22 (SSH) que permite escalación de privilegios. Tratamiento: Configuración de autenticación por clave.
- **Riesgo medio**: Vulnerabilidad en versiones obsoletas de Apache y MySQL. Tratamiento: Actualización a versiones seguras.

3.5 Medidas Correctivas

- **Deshabilitación de Servicios No Esenciales**: Deshabilitar FTP o usar FTPS/SFTP para proteger las credenciales transmitidas.

- **Autenticación en SSH**: Configuración de autenticación con claves SSH, eliminando acceso directo al root.

- **Control de acceso en bases de datos**: Restricción de MySQL a localhost.

---

4. Políticas de Seguridad de la Información

4.1 Política de Acceso a la Información

Solo los usuarios autorizados tendrán acceso a datos sensibles, mediante autenticación multifactor (MFA) en cuentas administrativas y políticas de contraseñas seguras.

4.2 Política de Uso de Activos y Recursos

Cada activo de información debe ser usado de acuerdo con las políticas establecidas, asegurando la no divulgación de información crítica.

4.3 Política de Cifrado de Datos Sensibles

Los datos sensibles serán cifrados en reposo y en tránsito. El cifrado en reposo utilizará algoritmos como AES-256, mientras que el cifrado en tránsito se gestionará mediante SSL/TLS.

4.4 Política de Respaldo de Información

- **Frecuencia de respaldo**: Diaria para datos críticos y semanal para datos de menor criticidad.

- **Tipología de respaldo**: Se utilizarán respaldos completos cada semana y respaldos incrementales diarios.

- **Pruebas de restauración**: Trimestralmente, para asegurar la integridad de los datos de respaldo.

4.5 Política de Actualización y Mantenimiento

- **Actualización continua**: Todos los paquetes y aplicaciones deben mantenerse en sus versiones más seguras.

- **Automatización**: Se establecerán actualizaciones automáticas para parches críticos usando herramientas de administración como unattended-upgrades en Debian.

---

5. Controles Técnicos y Administrativos

5.1 Control de Acceso Basado en Roles (RBAC)

Implementación de RBAC, asignando permisos según roles específicos en la organización, limitando el acceso a solo aquellos que necesitan los datos para su función.

5.2 Autenticación Multifactor (MFA)

MFA es obligatorio en accesos a sistemas críticos, especialmente para cuentas administrativas, añadiendo una capa de protección en los accesos remotos.

5.3 Firewalls y Configuraciones de Red

Se implementará un firewall (UFW) configurado para restringir puertos y protocolos a solo aquellos necesarios, limitando el acceso a servicios sensibles.

5.4 Seguridad de Servicios de Red y Bases de Datos

- **Configuración de MySQL**: Acceso limitado a conexiones internas (localhost) y requerimiento de contraseñas seguras para cada usuario de base de datos.

- **Ajustes en Apache y HTTP**: Configuración de permisos de acceso y protección contra vulnerabilidades CSRF y XSS mediante encabezados de seguridad como X-Frame-Options y Content-Security-Policy.

---

6. Procedimientos de Monitoreo y Detección de Actividades Anómalas

6.1 Herramientas de Monitoreo de Intrusiones

Se utiliza un sistema de detección de intrusiones (IDS) como Snort o Suricata para identificar accesos no autorizados y patrones de tráfico sospechosos en puertos críticos (ej., 22, 80, 3306).

6.2 Monitoreo de Registros de Seguridad

Implementación de herramientas como Splunk para la administración y revisión de registros de seguridad, auditando eventos inusuales y fallos de inicio de sesión en sistemas sensibles.

6.3 Alertas y Notificaciones

Configuración de alertas automáticas para eventos críticos en cuentas de alta jerarquía (ej., accesos de root), permitiendo al equipo de seguridad responder rápidamente a accesos no autorizados.

---

7. Planes de Respuesta a Incidentes

7.1 Identificación y Clasificación de Incidentes

Implementación de herramientas de monitoreo continuo como Nessus y Lynis para detectar vulnerabilidades, generando alertas automáticas para incidentes de alta prioridad.

7.2 Contención y Aislamiento

Para incidentes graves, el equipo debe aislar dispositivos afectados de la red y bloquear temporalmente accesos a servicios comprometidos (ej., SSH o FTP)

7.3 Erradicación y Recuperación

- **Erradicación de archivos maliciosos**: Escaneo completo con herramientas como rkhunter y chkrootkit para eliminar artefactos sospechosos.

- **Restauración de configuraciones**: Recuperación de configuraciones y eliminación de cambios en servicios comprometidos

7.4 Generación de Informes Post-Incidente

Documentación del incidente con detalles de las causas, acciones tomadas y recomendaciones de mejora. Este informe se utilizará para ajustar políticas y fortalecer la seguridad futura.

---

8. Capacitación y Concientización en Seguridad

8.1 Entrenamiento en Buenas Prácticas de Seguridad

Para fortalecer la seguridad en la organización, todos los empleados deben recibir entrenamiento sobre buenas prácticas de seguridad. Este programa incluirá:

- **Políticas de contraseñas seguras**: Cómo crear contraseñas robustas y mantenerlas en secreto.
- **Uso seguro de aplicaciones**: Indicaciones sobre la apertura de enlaces de fuentes confiables y el manejo de adjuntos en correos electrónicos.
- **Reconocimiento de amenazas de phishing**: Señales de advertencia de intentos de phishing y la importancia de no hacer clic en enlaces sospechosos.

Ejemplo de Contenido de Capacitación:

- **Simulacros de phishing**: Ejercicios prácticos en los que se envían correos electrónicos simulados de phishing para evaluar la capacidad de respuesta y aumentar la conciencia de los usuarios.
- **Capacitación mensual en seguridad de la información**: Una sesión de capacitación para revisar las políticas de la organización y reforzar las mejores prácticas.

8.2 Simulacros de Respuesta a Incidentes

La organización debe realizar simulacros de respuesta a incidentes para que el equipo esté preparado para actuar en caso de una amenaza real. Estos simulacros ayudan a familiarizar al equipo de TI y seguridad con el protocolo de respuesta y optimizar el tiempo de reacción ante un incidente.

Ejemplo de Simulacro:

- **Ataque de fuerza bruta en el servidor SSH**: Se simula un intento de fuerza bruta en el acceso SSH de un servidor. El equipo de seguridad debe identificar la amenaza, aislar el servicio afectado y documentar cada paso de la respuesta para ajustar las políticas según el resultado del simulacro.

8.3 Campañas de Concientización en Seguridad

Además de las capacitaciones específicas, es fundamental realizar campañas de concientización que mantengan a todos los empleados informados sobre temas de ciberseguridad. Estas campañas pueden incluir:

- **Boletines mensuales**: Informes de seguridad que resuman las amenazas más recientes y recomendaciones sobre prácticas de seguridad.
- **Carteles informativos en áreas comunes**: Recordatorios sobre prácticas seguras en el uso de correos y dispositivos de la organización.

---

9. Evaluación y Mejora Continua

La mejora continua es un pilar fundamental en el SGSI. Para asegurar que la organización se mantiene protegida y en cumplimiento con ISO 27001, es necesario realizar auditorías, evaluaciones regulares y ajustes a las políticas.

9.1 Auditorías Internas de Seguridad

Las auditorías internas ayudan a verificar la implementación y efectividad de los controles del SGSI. La auditoría debe incluir:

- **Revisión de cumplimiento de políticas**: Verificación de que las políticas de acceso, cifrado, y respaldo se siguen conforme al plan de seguridad.
- **Pruebas de penetración**: Ejecución de pruebas de penetración en servicios críticos como SSH, HTTP y bases de datos para detectar posibles vulnerabilidades.
- **Evaluación de registros y actividades de usuarios**: Verificación de los accesos y actividades de usuarios en servicios críticos para identificar actividades sospechosas.

9.2 Revisión y Ajuste de Políticas de Seguridad

Una vez concluida la auditoría, se debe realizar una revisión exhaustiva de las políticas de seguridad para identificar áreas de mejora y ajustes necesarios. Esto incluye:

- **Actualización de las políticas de acceso y autenticación**: Basado en los resultados de la auditoría, se podrían establecer nuevas reglas de acceso o implementar mejoras en autenticación, como MFA en todos los accesos críticos.
- **Ajuste en la configuración de respaldo y cifrado**: Verificar que los datos críticos estén protegidos mediante cifrado en reposo y en tránsito, y que los respaldos se almacenen en ubicaciones seguras.

9.3 Monitoreo y Evaluación Continua

La implementación de sistemas de monitoreo en tiempo real permitirá detectar incidentes rápidamente y tomar medidas preventivas antes de que se conviertan en amenazas serias. El monitoreo continuo debe abarcar:

- **Análisis en tiempo real de registros y tráfico de red**: Uso de herramientas de monitoreo como Splunk para revisar logs y alertar sobre patrones anómalos en el tráfico de red.
- **Revisión periódica de permisos de usuario**: Asegurarse de que solo los usuarios autorizados accedan a información sensible, ajustando permisos en función de las necesidades actuales de la organización.

9.4 Evaluación de Incidentes y Lecciones Aprendidas

Cada incidente o simulacro debe documentarse para revisar y aprender de la experiencia. Este análisis permitirá a la organización ajustar el SGSI continuamente. El proceso incluye:

- **Informe de lecciones aprendidas**: Un reporte con el análisis del incidente, las respuestas ejecutadas y las áreas de mejora detectadas.
- **Actualización del plan de respuesta a incidentes**: Ajustes a los protocolos de respuesta para aumentar la efectividad ante futuros incidentes similares.

---

10. Mecanismos de Protección de Datos

Para proteger la integridad y disponibilidad de la información, se implementarán mecanismos de seguridad basados en las mejores prácticas, como respaldos periódicos, cifrado, controles de acceso y monitoreo continuo.

10.1 Respaldo de Datos Periódico

El respaldo de información es fundamental para asegurar que, en caso de incidente, la organización pueda recuperar los datos críticos.

- **Frecuencia de Respaldo**: Se realizarán respaldos diarios para datos críticos y semanales para información de menor importancia.
- **Tipología de Respaldo**: Los respaldos completos se realizarán una vez a la semana, con respaldos incrementales diarios.
- **Almacenamiento Seguro de Respaldo**: Los respaldos se almacenarán en ubicaciones físicas separadas de la red de producción, y se cifrarán para evitar accesos no autorizados.

10.2 Cifrado de Datos Sensibles

- **Cifrado de Datos en Reposo**: Se aplicará cifrado AES-256 para toda información almacenada en bases de datos y servidores que contengan datos sensibles.

- **Cifrado de Datos en Tránsito**: Las conexiones de datos sensibles, como las de MySQL y servicios HTTP, deberán contar con cifrado SSL/TLS para proteger la información mientras se transfiere.

- **Gestión de Claves**: Las claves de cifrado se gestionarán mediante un sistema de control de claves, como un módulo de seguridad de hardware (HSM), para asegurar que se almacenen de manera segura y que se roten periódicamente.

10.3 Controles de Acceso Estrictos

- **Control de Acceso Basado en Roles (RBAC)**: Se limitarán los permisos de cada usuario según su rol y responsabilidad dentro de la organización, minimizando la exposición de datos sensibles.

- **Autenticación Multifactor (MFA)**: El acceso a sistemas críticos se realizará con autenticación MFA, protegiendo las cuentas con acceso privilegiado.

- **Políticas de Contraseñas Seguras**: Todos los usuarios deberán cumplir con requisitos de contraseñas fuertes, renovando estas periódicamente.

10.4 Monitoreo y Detección de Actividades Anómalas

- **Sistema de Detección de Intrusiones (IDS)**: Implementación de un IDS para monitorear en tiempo real el tráfico de red y alertar sobre patrones sospechosos.

- **Monitoreo de Logs de Seguridad**: Uso de herramientas como ELK Stack para centralizar y analizar registros de seguridad, identificando patrones anómalos de acceso y alertando al equipo de seguridad.

- **Alertas en Cuentas de Alta Privilegio**: Configuración de alertas para accesos y modificaciones en cuentas administrativas, de modo que se detecten actividades sospechosas de manera inmediata.

10.5 Política de Respaldo y Recuperación de Datos

El respaldo de datos es esencial para mantener la continuidad de las operaciones en caso de incidentes de seguridad. La organización implementará una política de respaldo que abarque:

- Frecuencia y tipos de respaldo: Se utilizarán respaldos completos semanales y respaldos incrementales diarios.

- Pruebas de restauración: Se realizarán pruebas de restauración trimestrales para asegurar que los datos respaldados pueden recuperarse en caso de ser necesario.

---

11. Apéndice

11.1 Anexos de Documentación

1. Políticas de Seguridad de la Información

Estas políticas son directrices generales que definen cómo debe manejarse la seguridad de la información en la organización. Algunos ejemplos que puedes incluir son:

- **Política de Acceso a la Información**: Define quién tiene permiso para acceder a ciertos datos y sistemas. Describe los niveles de acceso (por ejemplo, usuario, administrador) y los métodos de autenticación.
- **Política de Uso Aceptable de Activos**: Especifica las prácticas de uso aceptable de equipos y redes, incluidas restricciones sobre el acceso y la descarga de contenido no autorizado o inapropiado.
- **Política de Cifrado de Datos**: Establece cuándo y cómo deben cifrarse los datos en reposo y en tránsito, especificando los algoritmos de cifrado y los protocolos de transmisión (por ejemplo, TLS/SSL).
- **Política de Contraseñas**: Define los requisitos de complejidad de contraseñas, la frecuencia de cambio y el manejo seguro de credenciales. También puede incluir la obligatoriedad de autenticación multifactor para ciertos accesos.
- **Política de Respaldo y Recuperación de Datos**: Indica la frecuencia, tipo de respaldo (completo, incremental) y almacenamiento seguro de los respaldos. Incluye procedimientos de prueba de restauración.
- **Política de Actualización de Software y Parches**: Establece los lineamientos para mantener todos los sistemas y aplicaciones actualizados con parches de seguridad para reducir vulnerabilidades.
- **Política de Uso de Dispositivos Móviles**: Describe las normas de seguridad para dispositivos móviles, incluyendo cifrado, autenticación y protección de datos.

2. Procedimientos de Respuesta a Incidentes

Un conjunto de procedimientos de respuesta a incidentes ayuda a gestionar de forma estructurada cualquier evento de seguridad. Ejemplos de procedimientos que podrías incluir:

- **Procedimiento de Identificación y Notificación de Incidentes**: Define cómo deben identificarse, clasificarse y notificarse los incidentes de seguridad, incluyendo ejemplos de eventos que deben reportarse.
- **Procedimiento de Contención y Aislamiento**: Describe los pasos para contener un incidente y aislar los sistemas afectados para evitar su propagación. Puede incluir configuraciones específicas de firewall o directrices para desconectar equipos de la red.

- **Procedimiento de Erradicación y Recuperación**: Indica los pasos para eliminar la causa del incidente y restaurar los sistemas a su estado seguro. Puede incluir procedimientos de restauración de respaldo y configuraciones de seguridad reforzadas.
- **Procedimiento de Generación de Informes de Incidentes**: Plantilla para documentar cada incidente con detalles sobre su detección, impacto, respuesta y lecciones aprendidas. Esto facilita el análisis posterior y la mejora continua.

3. Configuraciones de Seguridad de Sistemas y Herramientas

Documentar las configuraciones de seguridad específicas garantiza que los sistemas clave se configuren de manera uniforme y segura. Algunos ejemplos:

- **Configuración de Firewalls**: Instrucciones sobre cómo configurar reglas de firewall para restringir el acceso a puertos y servicios críticos. Incluye ejemplos de comandos o scripts de configuración (por ejemplo, usando iptables o UFW en Linux).
- **Configuración de Autenticación Multifactor (MFA)**: Paso a paso para habilitar MFA en sistemas críticos (ej., acceso a la VPN, bases de datos y consolas de administración). Especifica qué métodos de MFA se requieren (SMS, app autenticadora, etc.).
- **Configuración de IDS/IPS (Sistemas de Detección/Prevención de Intrusiones)**: Guía de instalación y configuración de un IDS/IPS, como Snort o Suricata, incluyendo reglas de monitoreo y alertas para detectar actividad inusual.
- **Configuración de Monitoreo de Logs**: Proceso de instalación y configuración de herramientas de monitoreo de logs (por ejemplo, Splunk o ELK Stack), incluyendo los logs que deben monitorearse y cómo configurar alertas automáticas para eventos críticos.
- **Configuración Segura de Servidores Web (Apache, Nginx)**: Directrices para la configuración segura de servidores web, incluyendo headers de seguridad como X-Frame-Options, X-Content-Type-Options, y Content-Security-Policy.

4. Procedimientos de Gestión de Riesgos

Para gestionar eficazmente los riesgos, necesitas procedimientos que describan el ciclo completo de gestión de riesgos. Ejemplos:

- **Procedimiento de Evaluación de Riesgos**: Guía para identificar, evaluar y clasificar riesgos. Esto incluye cómo se realizan las entrevistas, qué información debe recopilarse y cómo se calcula el riesgo en términos de probabilidad e impacto.
- **Procedimiento de Tratamiento de Riesgos**: Describe las opciones para tratar los riesgos identificados (evitar, mitigar, transferir o aceptar) y detalla los pasos para implementar controles específicos.

- **Matriz de Riesgos y Controles**: Tabla para documentar cada riesgo con su clasificación de severidad y los controles aplicados para su mitigación.

5. Plantillas y Formularios

Las plantillas ayudan a estandarizar la recopilación de datos y documentación en torno a la seguridad. Ejemplos de plantillas útiles incluyen:

- **Plantilla de Evaluación de Riesgos**: Formulario para documentar el riesgo, incluyendo descripción, probabilidad, impacto y controles propuestos.
- **Plantilla de Informe de Incidentes**: Documento para registrar los detalles de un incidente de seguridad, como la descripción, los activos afectados, el impacto, la respuesta y las medidas de mitigación adoptadas.
- **Plantilla de Registro de Accesos**: Formato para registrar y monitorear los accesos a áreas o sistemas críticos, especificando quién accedió, a qué hora y el propósito.

6. Procedimientos de Auditoría y Cumplimiento

Para verificar que el SGSI está cumpliendo con las políticas establecidas, los procedimientos de auditoría y cumplimiento son fundamentales:

- **Procedimiento de Auditoría Interna de Seguridad**: Guía para planificar, ejecutar y documentar auditorías de seguridad interna. Incluye los controles que deben revisarse y los criterios de evaluación.
- **Lista de Verificación de Cumplimiento de Políticas de Seguridad**: Un checklist para asegurar que todas las políticas del SGSI se están siguiendo. Puede incluir preguntas de verificación sobre acceso a sistemas, actualización de software, cifrado de datos, etc.

11.2 Glosario de Términos Técnicos

- **Confidencialidad**: Garantía de que la información es accesible solo para las personas autorizadas.

- **Integridad**: Asegurarse de que la información y los métodos de procesamiento son exactos y completos.

- **IDS (Intrusion Detection System)**: Sistema de detección de intrusiones que supervisa el tráfico de la red o los eventos del sistema en busca de actividades maliciosas.

- **MFA (Multi-Factor Authentication)**: Método de autenticación que requiere múltiples factores de verificación para acceder a un recurso.

- **Política de Cifrado**: Directrices que especifican cómo debe realizarse el cifrado de datos para proteger la información.

11.3 Referencias

1.- **Normas y Estándares**:

- **ISO/IEC 27001**: Norma internacional para sistemas de gestión de seguridad de la información.
- **ISO/IEC 27002**: Guía de controles de seguridad de la información.
- **NIST SP 800-61**: Guía de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU.