IMPLEMENTACIÓN SGSI EMPRESA 4GEEKS

ALEJANDRO GIL SÁNCHEZ

Implementación SGSI Empresa 4GEEKS

INFORME DE SGSI

1. Introducción 2
   1.1 Objetivo del documento 2
   1.2 Contexto del servidor comprometido 2
   1.3 Rol del equipo IT y necesidad del SGSI 2
2. Plan de Respuesta a Incidentes (basado en NIST SP 800-61) 3
   2.1 Fases del Ciclo de Respuesta 3
   2.2 Clasificación y severidad de incidentes 4
   2.3 Roles y responsabilidades 4
3. Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) 4
   3.1 Política de Seguridad de la Información 4
   3.2 Análisis y gestión de riesgos (basado en ISO 27005) 5
   3.3 Controles recomendados según Anexo A de ISO/IEC 27001 5
   3.4 Planes de acción correctiva 5
4. Medidas Técnicas y de Prevención 5
   4.1 Prevención de pérdida de datos (DLP) 5
   4.2 Backups y recuperación ante desastres 6
   4.3 Herramientas recomendadas 6
5. Conclusión 6

1. Introducción

1.1 Objetivo del documento

El presente informe tiene como objetivo diseñar un Plan de Respuesta ante Incidentes de Seguridad y un Sistema de Gestión de Seguridad de la Información (SGSI) para una organización que ha sufrido un ciberataque. Este plan permitirá responder eficazmente ante futuros incidentes, mitigar sus impactos y establecer controles para prevenir su recurrencia, basándose en los estándares NIST SP 800-61 e ISO/IEC 27001.

1.2 Contexto del servidor comprometido

Durante las fases previas del proyecto, se analizó un servidor Debian comprometido que formaba parte de una infraestructura crítica de la organización 4Geeks Academy. El servidor fue vulnerado a través de varios vectores: acceso vía SSH con contraseñas débiles, FTP anónimo, y un WordPress desactualizado con configuraciones inseguras. Estas intrusiones permitieron al atacante escalar privilegios y modificar configuraciones críticas del sistema.

1.3 Rol del equipo IT y necesidad del SGSI

La organización cuenta con un equipo de IT básico sin roles dedicados a ciberseguridad. Ante este escenario, se hace imprescindible establecer procedimientos formales de seguridad y respuesta ante incidentes que aseguren la continuidad del negocio, la integridad de la información y la confidencialidad de los datos gestionados.

2. Plan de Respuesta a Incidentes (basado en NIST SP 800-61)

2.1 Fases del Ciclo de Respuesta

Preparación:

- Inventariado de activos críticos.
- Establecimiento de responsables (aunque sea un equipo reducido).
- Instalación de herramientas de monitoreo y detección como Wazuh.
- Procedimientos de backup y restauración.
- Concienciación en ciberseguridad.

Identificación:

- Análisis de logs del sistema, herramientas SIEM.
- Alertas de comportamiento anómalo en conexiones o procesos.
- Uso de sistemas de detección de intrusiones (IDS).

Contención:

- Aislamiento del sistema afectado.
- Cambio inmediato de credenciales comprometidas.
- Desactivación temporal de servicios vulnerables.

Erradicación:

- Eliminación de puertas traseras, scripts persistentes y usuarios no autorizados.
- Restauración de permisos originales.

Recuperación:

- Restaurar la funcionalidad desde una copia segura.
- Verificar integridad con herramientas de validación (ej. checksums).

Lecciones aprendidas:

- Documentar lo sucedido.
- Mejorar los controles de seguridad.
- Simular nuevos escenarios para preparar al equipo.

2.2 Clasificación y severidad de incidentes

Tabla de Tipos de Incidente

Tipo de Incidente	Severidad	Tiempo de respuesta	Responsable
Acceso no autorizado (SSH)	Crítico	Inmediato	Administrador de red
Malware detectado	Alto	< 1 hora	Encargado de sistemas
Fuga de información	Crítico	Inmediato	Responsable IT
Análisis de vulnerabilidad	Medio	< 24 horas	Equipo IT

2.3 Roles y responsabilidades

Dado que el equipo es reducido, se asignan funciones concretas:

Tabla de Roles y Funciones

Rol	Funciones clave
Responsable de seguridad	Coordina la respuesta, toma decisiones técnicas
Admin. sistemas / redes	Aplica mitigaciones, analiza logs, ejecuta acciones
Responsable de documentación	Recoge evidencias, redacta informes
Usuario designado	Contacto de comunicación con usuarios o afectados

3. Diseño del Sistema de Gestión de Seguridad de la Información (SGSI)

3.1 Política de Seguridad de la Información

- La política debe reflejar el compromiso de la organización con la protección de sus activos. Incluirá:
- Confidencialidad: solo personal autorizado accede a los datos.
- Integridad: asegurar que los datos no se modifican sin control.
- Disponibilidad: los recursos deben estar disponibles cuando se necesiten.

Ejemplo de declaración:

"La dirección de 4Geeks Academy se compromete a establecer y mantener un SGSI conforme a la norma ISO/IEC 27001 con el objetivo de garantizar la protección de los activos de información y el cumplimiento normativo."

3.2 Análisis y gestión de riesgos (basado en ISO 27005)

Se realiza un análisis de riesgos para detectar vulnerabilidades y amenazas.

Tabla de Evaluación de Riesgos

Activo Crítico	Amenaza	Riesgo potencial	Nivel de riesgo
Servidor web	Explotación de RCE	Pérdida total de control del sistema	Alto
Base de datos	Fuga de credenciales	Exposición de datos sensibles	Crítico
FTP sin cifrado	Interceptación de tráfico	Robo de credenciales	Alto

3.3 Controles recomendados según Anexo A de ISO/IEC 27001

Tabla de Controles ISO 27001 y Medidas Aplicadas

Control (ISO A.5–A.18)	Medida aplicada
A.9 Control de accesos	Implementar autenticación multifactor
A.10 Cifrado	Uso de HTTPS y cifrado de datos sensibles
A.12 Protección contra malware	Software antivirus actualizado regularmente
A.16 Gestión de incidentes	Plan de respuesta implementado
A.17 Continuidad del negocio	Procedimientos de recuperación definidos

3.4 Planes de acción correctiva

Tras la implementación inicial, se definen acciones de seguimiento para mantener y mejorar el SGSI:

- Auditorías internas periódicas.
- Revisión y actualización anual del análisis de riesgos.
- Revisión de logs semanales.
- Simulacros de respuesta ante incidentes cada 6 meses.

4. Medidas Técnicas y de Prevención

4.1 Prevención de pérdida de datos (DLP)

- Establecimiento de permisos de acceso por rol (principio de mínimo privilegio).
- Prohibición de dispositivos USB sin autorización.
- Cifrado de unidades de disco.
- Monitoreo de transferencias externas.

4.2 Backups y recuperación ante desastres

- Backups automáticos diarios.
- Almacenamiento cifrado en repositorios locales y externos.
- Pruebas de restauración de backups cada trimestre.

4.3 Herramientas recomendadas

- Wazuh para monitoreo y respuesta ante incidentes.
- Fail2ban para bloquear IPs tras múltiples intentos fallidos.
- ClamAV como antivirus.
- rkhunter y chkrootkit para detectar rootkits.

5. Conclusión

Tras un análisis profundo del servidor comprometido, se evidenció que las principales causas del ataque fueron una falta de medidas básicas de protección, uso de credenciales débiles, y servicios inseguros habilitados sin control. Este informe propone un marco completo de actuación que combina la respuesta ante incidentes con la prevención a través de un SGSI conforme a ISO/IEC 27001.

Implementar este plan permitirá a la organización reducir significativamente su superficie de ataque, responder de forma estructurada ante futuros incidentes y alinear sus políticas con estándares internacionales. Esta experiencia demuestra la necesidad urgente de profesionalizar la seguridad incluso en entornos con recursos limitados, apostando por procedimientos, automatización, y una cultura organizativa orientada a la prevención.