Sistema de Gestión de Seguridad de la Información (SGSI) Basado en ISO/IEC 27001 Proyecto Final

1. Introducción

Este documento presenta un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, aplicado al caso de estudio de un servidor Debian comprometido debido a vulnerabilidades en SSH y WordPress. El objetivo del SGSI es garantizar la seguridad de la información y la continuidad operativa mediante la implementación de controles y buenas prácticas.

2. Alcance del SGSI

Este SGSI abarca:

- La infraestructura de TI del servidor Debian.
- La configuración y administración del servicio SSH.
- La plataforma WordPress alojada en el servidor.
- Los accesos remotos y autenticación de usuarios.
- La gestión de incidentes de seguridad.

Se excluyen otros servicios como FTP, Apache y MariaDB, que serán abordados en informes separados.

3. Política de Seguridad de la Información

El objetivo de esta política es proteger la información y los sistemas contra accesos no autorizados, garantizando su integridad, confidencialidad y disponibilidad.

Principios fundamentales:

- Aplicar controles de seguridad según ISO 27001.
- Implementar medidas de protección contra amenazas internas y externas.
- Mantener actualizado el software y configuraciones seguras.
- Realizar auditorías y pruebas de seguridad periódicas.

4. Análisis y Evaluación de Riesgos

Se identifican los siguientes riesgos clave:

ID	Riesgo	Impacto	Probabilidad	Nivel de Riesgo
001	Acceso no autorizado por configuración insegura de SSH	Alto	Alta	Crítico
002	Ataque de fuerza bruta a WordPress	Alto	Alta	Crítico
003	Indexación de archivos sensibles en WordPress	Medio	Media	Medio
004	Uso de credenciales por defecto	Alto	Alta	Crítico

5. Controles de Seguridad Basados en ISO 27001

Se establecen controles de seguridad según los dominios de ISO 27001:

- **A.9 Control de Acceso**
  - Implementación de autenticación de dos factores (2FA).
  - Restricción de accesos a usuarios autorizados.
- **A.12 Seguridad de las Operaciones**
  - Monitoreo de accesos y registros de actividad.
  - Uso de IDS/IPS para detectar accesos no autorizados.
- **A.13 Seguridad en las Comunicaciones**
  - Implementación de cifrado en las conexiones SSH y web.
- **A.14 Seguridad de Desarrollo y Mantenimiento**
  - Aplicación de actualizaciones de software de manera regular.

6. Procedimientos de Seguridad para SSH y WordPress

Para mitigar vulnerabilidades, se implementan las siguientes medidas:

6.1 Configuración Segura de SSH

- Deshabilitar el acceso root mediante `PermitRootLogin no`.
- Restringir acceso a IPs específicas.
- Usar autenticación con claves en lugar de contraseñas.

6.2 Seguridad en WordPress

- Deshabilitar la indexación de archivos con `robots.txt`.
- Implementar plugins de seguridad como Wordfence o Sucuri.
- Aplicar políticas de contraseñas seguras.

7. Monitoreo y Auditoría de Seguridad

Se deben realizar auditorías periódicas con herramientas como:

- **Nmap:** Para escaneo de puertos.
- **Metasploit:** Para pruebas de penetración.
- **Rkhunter:** Para detección de rootkits.
- **Fail2Ban:** Para bloquear intentos de acceso sospechosos.

Además, se recomienda la creación de una **base de datos de incidentes**, donde se registren todos los casos de seguridad detectados, junto con su resolución. Esto permitirá un análisis histórico de eventos y mejorar la respuesta ante futuras amenazas.

8. Plan de Respuesta ante Incidentes

En caso de incidente, se aplicarán los siguientes pasos:

1. **Detección:** Identificación del evento sospechoso.
2. **Contención:** Bloqueo de accesos y restricciones temporales.
3. **Erradicación:** Eliminación de amenazas y reparación de vulnerabilidades.
4. **Recuperación:** Restauración de sistemas desde respaldos seguros.
5. **Lecciones Aprendidas:** Documentación del incidente y mejora de controles.

9. Plan de Mejora Continua

Para mantener el SGSI efectivo, se aplicará el ciclo PDCA (Plan-Do-Check-Act):

- **Plan:** Identificar y analizar riesgos.
- **Do:** Implementar controles de seguridad.
- **Check:** Auditar y monitorear regularmente.
- **Act:** Mejorar procesos y actualizar controles.

10. Conclusión

El presente SGSI proporciona un enfoque estructurado y basado en estándares para mitigar riesgos de seguridad en el servidor Debian afectado. La aplicación de las políticas y controles descritos reducirá significativamente la posibilidad de ataques y mejorará la postura de seguridad de la organización. Se recomienda la ejecución constante de auditorías y la actualización del SGSI para enfrentar nuevas amenazas.