# Implementación Extendida de un SGSI basado en ISO 27001

## 1. Contexto Inicial

El servidor Debian (IP 10.0.2.11) presentaba múltiples vulnerabilidades detectadas tras un proceso de pentesting y análisis forense. Se identificaron accesos no autorizados a través de SSH utilizando credenciales válidas, bases de datos con contraseñas débiles, servicios innecesarios (FTP vulnerable), y configuraciones inseguras en el sistema de gestión de contenido WordPress, como permisos de archivos y carpetas completamente abiertos (777).

## 2. Objetivo del SGSI

El objetivo es establecer un sistema robusto de gestión de seguridad de la información que garantice la protección de los activos críticos de información, minimice los riesgos de accesos no autorizados y asegure la capacidad de respuesta ante incidentes, cumpliendo con las buenas prácticas internacionales definidas por la norma ISO/IEC 27001.

## 3. Alcance del SGSI

El SGSI incluye:
- Infraestructura de servidores (Debian, Apache, MariaDB, WordPress).
- Sistemas de acceso remoto (SSH, VPN).
- Servicios de red y gestión de tráfico.
- Almacenamiento de credenciales y bases de datos.
- Sistemas de logs y monitorización.
- Personal técnico con acceso privilegiado.

## 4. Análisis de Riesgos

Se realizó un análisis detallado basado en ISO 27005 considerando:
- Amenazas internas y externas.
- Vulnerabilidades técnicas (contraseñas débiles, servicios expuestos, permisos inseguros).
- Impacto sobre la confidencialidad, integridad y disponibilidad de la información.
- Evaluación de probabilidades de explotación.

Resultado: varios riesgos críticos identificados, especialmente en accesos SSH, FTP vulnerable y permisos en WordPress.

## 5. Políticas de Seguridad Definidas

Se definieron políticas específicas, incluyendo:

- Gestión de accesos: SSH solo con claves públicas, prohibido acceso root remoto, mínimo privilegio.
- Gestión de vulnerabilidades: actualizaciones automáticas, revisiones mensuales de parches, auditorías trimestrales.
- Protección de aplicaciones web: revisión de permisos, escaneos periódicos de vulnerabilidades web.
- Continuidad del negocio: backups automatizados, simulacros de recuperación, procedimientos documentados.
- Monitorización centralizada: implementación de SIEM para correlación de eventos.
- Formación continua: capacitación periódica para personal técnico y usuarios.

## 6. Plan de Acción Detallado

Se establece un cronograma de acciones:
- Inmediato: bloqueo SSH por IP, eliminación de FTP, cambios de contraseñas.
- 1 mes: auditoría de permisos WordPress, implementación inicial de SIEM, deshabilitar accesos inseguros.
- 3 meses: completar despliegue de SIEM, revisión completa de políticas de seguridad.
- 6 meses: simulacros de recuperación de desastres y auditorías de continuidad.
- Anualmente: formación continua, revisión integral de riesgos y políticas.

## 7. Ciclo de Mejora Continua (PDCA)

El SGSI sigue el ciclo Plan-Do-Check-Act:
- PLAN: identificar activos y riesgos, definir políticas.
- DO: implementación de controles.
- CHECK: auditorías periódicas, revisión de incidentes.
- ACT: aplicar medidas correctivas, actualizar el SGSI constantemente.

## 8. Conclusiones Finales

La implementación de este SGSI permitirá establecer controles formales y documentados, reducir la superficie de ataque, asegurar el cumplimiento de

normativas, mejorar la capacidad de respuesta ante incidentes y fortalecer la seguridad global de la organización de forma sostenible y profesional.