Resumen de enfoque SGSI 4Geeks Academy

Valentina Alcubillas Arango - 04/02/2026
4Geeks Academy
Basado en ISO/IEC 27001:2022

Introducción SGSI

¿Qué es un SGSI?

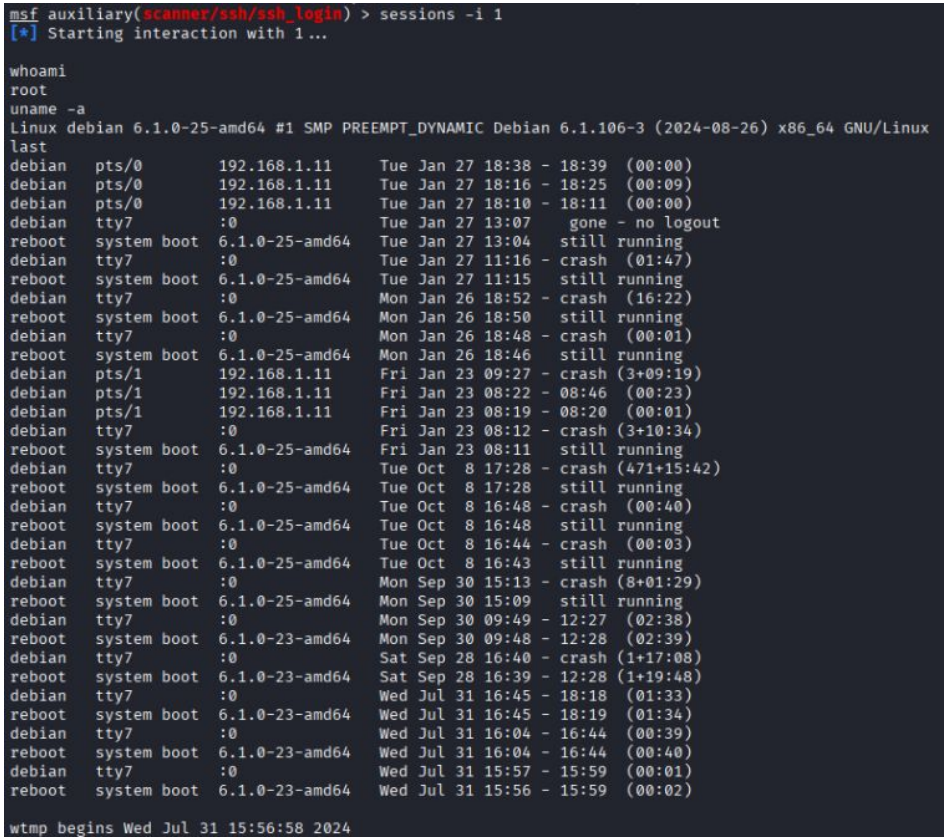
- Marco para proteger la información
- Enfoque en Confidencialidad, Integridad y Disponibilidad (CIA)
- Seguridad como proceso continuo

Es un **marco estructurado** y **sistemático** que permite a una organización gestionar **eficientemente** la seguridad de su información.

La implantación responde a la necesidad de **gestionar riesgos** asociados a la **información** de la organización educativa, además de reforzar la **confianza** de la comunidad estudiantil, público en general y proveedores frente a vulnerabilidades ⚠️.

Vulnerabilidad SSH

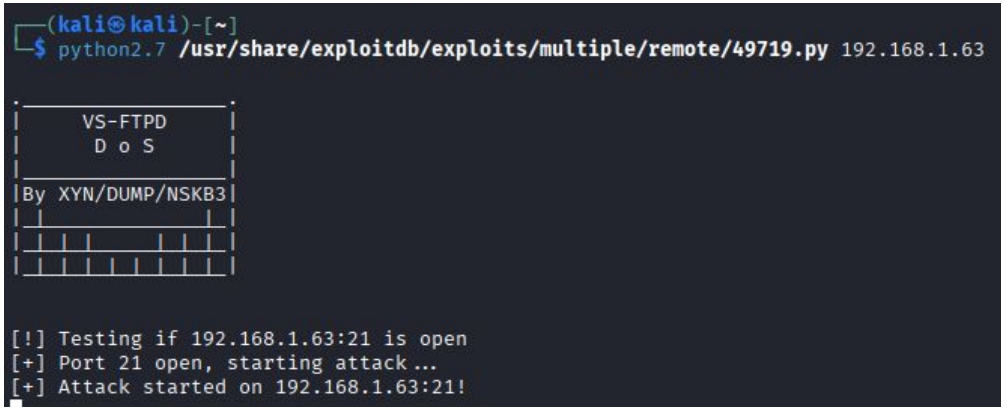
- Debian OpenSSL Predictable PRNG vulnerability (Fuerza bruta SSH)
- EDB-ID: 5622
- CVE: 2008-0166
- Tipo: Remoto



Siguiente vulnerabilidad 🌸

Vulnerabilidad vsftpd 3.0.3

- DoS (Denial of Service)
- EDB ID: 49719
- Tipo: Remoto



Siguiente apartado🌸

Contexto organizativo

Contexto organizativo

- **Entorno Digital**: Operación internacional distribuida con alta dependencia en la nube.
- **Desafíos**: Mitigación de riesgos en datos personales, accesos remotos y disponibilidad.
- **Necesidad**: Gestión sistemática de riesgos para garantizar fiabilidad y cumplimiento.

Partes Interesadas:

- **Internas**: Dirección, equipo técnico, personal docente y administrativo.
- **Externas**: Estudiantes, proveedores tecnológicos, socios comerciales y organismos reguladores.

Compromiso de la Dirección:

- Provisión de recursos para el mantenimiento del sistema.
- Cultura de "Seguridad por Diseño" en el desarrollo de plataformas.
- Revisión anual contra amenazas emergentes (Ransomware e Ingeniería Social).

Alcance

Quedan excluidos del alcance los sistemas personales no autorizados y aquellos entornos no relacionados con la actividad educativa u operativa de la organización.

¿Qué protegemos?

- Plataformas educativas y gestión académica.
- Infraestructura en la nube y servicios web.
- Datos de estudiantes, docentes y personal.

¿Por qué?

- ***Confianza***: Asegurar la privacidad de alumnos y docentes.
- ***Continuidad***: Evitar interrupciones en el aprendizaje.
- ***Cumplimiento***: Alineación con estándares internacionales (ISO 27001).

Activos de información

Son el **conjunto de recursos críticos** (datos, software y personas) que permiten el **funcionamiento** y la **entrega** del valor educativo de **4Geeks**.

Activos esenciales:

- ***Información***: Registros académicos, materiales didácticos y claves de acceso.
- ***Software***: LMS (plataformas de aprendizaje) y repositorios de código.
- ***Infraestructura***: Servidores virtuales, redes y copias de seguridad.
- ***Factor Humano***: El equipo técnico y docente es la pieza clave en la prevención.

Roles y responsabilidades

- ***Dirección***: Aprueba políticas y dota de recursos.
- ***Responsable SGSI***: Supervisa el cumplimiento y gestiona riesgos.
- ***Equipo Técnico***: Implementa controles y mantiene la infraestructura.
- ***Usuarios (Staff/Alumnos):*** Cumplir con las políticas de uso aceptable.

Nota: En la segregación de funciones garantiza que quien opera no sea quien audita.

Controles seleccionados

- ***CTRL 01/02:*** Gestión estricta de identidades y "Mínimo Privilegio".
- ***CTRL 03/04***: Cifrado de datos y monitoreo de logs de actividad.
- ***CTRL 05***: Estrategia de backups y plan de recuperación ante desastres.
- ***CTRL 06***: Plan de concienciación y cultura de seguridad.

Herramientas Técnicas (DLP)

- **Symantec DLP**: Prevención de fuga de datos en la red (tráfico sensible).
- **Digital Guardian**: Control de endpoints para evitar la extracción de bases de datos MariaDB.
- **Protección de Datos**: Cifrado en reposo y en tránsito.

Respuesta a Incidentes (Marco NIST)

- ***Identificar***: Activos comprometidos (Servidor Debian).
- ***Proteger***: Cierre de puertos vulnerables y actualización de OpenSSL/vsftpd.
- ***Detectar***: Alertas tempranas ante picos de tráfico (DoS).
- ***Responder***: Protocolo de aislamiento de servidores afectados.
- ***Recuperar***: Restauración mediante backups limpios y seguros.

Indicadores SGSI

Indicador	Fuente de Medición	Frecuencia	Meta
Eficacia de Controles	Auditorías / Revisiones	Anual	100% cumplimiento de controles críticos.
Gestión de Incidentes	Registro de incidentes	Trimestral	Resolución del 100% de incidentes detectados.
Actualización de Riesgos	Evaluaciones de riesgos	Anual	0 riesgos "Críticos" sin plan de tratamiento.
Vigencia Documental	Manual y Políticas	Anual	100% de documentos revisados y firmados.
Disponibilidad del Servicio	SLA / Equipo Técnico	Continuo	Cumplimiento de los tiempos de respuesta definidos.

Mejora Continua (PDCA)

Seguridad = Proceso

- *Plan (Planificar)*
- *Do (Hacer)*
- *Check (Verificar)*
- *Act (Actuar)*

Anexo

- Riesgo de vulnerabilidades
- Exploit DB (base de datos de vulnerabilidades)
- Entidad educativa (4Geeks Academy)

Conclusiones

¿Preguntas?