

# **Presentación Ejecutiva — Incidente de Seguridad en Servidor Debian GNU/Linux**

## **Resumen ejecutivo para la dirección**

**Autor:** Alejandro Winter

**Contenido:** Este documento presenta una visión ejecutiva del incidente de seguridad detectado en un servidor Debian GNU/Linux, los riesgos asociados, las acciones correctivas aplicadas y las recomendaciones estratégicas para evitar su recurrencia.

## 2. RESUMEN EJECUTIVO

El presente informe recoge los resultados del análisis de seguridad realizado sobre un sistema Linux en un entorno de laboratorio, simulando una auditoría de ciberseguridad llevada a cabo por una empresa especializada en seguridad informática.

El objetivo principal del proyecto ha sido identificar vulnerabilidades de seguridad, analizar un incidente previamente detectado, evaluar el impacto potencial sobre el sistema y aplicar medidas correctivas orientadas a la mitigación de riesgos y a la mejora del nivel de seguridad global.

Durante la **Fase 1**, se llevó a cabo un análisis forense del sistema comprometido, identificando accesos no autorizados y configuraciones inseguras que permitían la explotación de servicios expuestos. A partir de este análisis, se aplicaron medidas de contención y mitigación para evitar la escalada de privilegios y reducir la superficie de ataque.

**La siguiente gráfica muestra la distribución de las vulnerabilidades identificadas durante el análisis, ponderadas según su severidad e impacto estimado en el entorno.**



- Acceso SSH inseguro -> 25% ●
- FTP con acceso anónimo -> 25% ●
- Puertos abiertos innecesarios -> 20% ○
- Permisos inseguros en wp-config.php -> 13,3% ○
- Directorio web listable -> 16,7% ○

---

En la **Fase 2**, se realizó un **proceso de pentesting** desde una máquina externa, simulando el comportamiento de un **atacante real**. Mediante técnicas de **escaneo y explotación** controlada, se detectaron **vulnerabilidades adicionales** que podrían haber sido aprovechadas para **comprometer el sistema**, las cuales fueron posteriormente **corregidas y validadas**.

Finalmente, en la **Fase 3**, se diseñó un plan de **respuesta a incidentes** y un conjunto de **medidas preventivas** alineadas con **buenas prácticas** y marcos de referencia como **NIST** e **ISO 27001**, con el fin de **fortalecer la seguridad del sistema** y mejorar la **capacidad de respuesta ante futuros incidentes**.

Como **resultado del análisis** y de las **acciones aplicadas**, el sistema evaluado presenta un **nivel de seguridad superior al inicial**, habiendo reducido significativamente los **riesgos detectados** y estableciendo una **base sólida** para la gestión de la **seguridad** en entornos similares.