INFORME EJECUTIVO DE GERENCIA

Incidente de Seguridad – Servidor Debian WordPress
Cliente: 4Geeks
Fecha: Febrero 2026
Clasificación: Confidencial

1. Resumen Ejecutivo

Durante el mes de febrero de 2026 se confirmó un **compromiso total de un servidor crítico Debian (LAMP Stack)** que alojaba servicios web (WordPress), SSH y FTP.

El incidente se originó por:

- Configuraciones inseguras (FTP anónimo habilitado).
- Contraseñas débiles (SSH y WordPress).
- Ausencia de controles formales de gobierno de seguridad.
- Falta de monitorización preventiva.

El atacante logró:

- Acceso inicial mediante FTP.
- Ataque de fuerza bruta por SSH.
- Escalada de privilegios a usuario root.
- Acceso a credenciales en texto plano de WordPress.
- Posible control completo del sistema.

Posteriormente se ejecutaron:

- Análisis forense digital (post-mortem).
- Auditoría de seguridad ofensiva (Pentesting).
- Plan de Hardening y mitigación.

- Evaluación GRC alineada con ISO 27001, National Institute of Standards and Technology (NIST CSF) y Centro Criptológico Nacional (ENS).

2. Impacto Empresarial

Riesgos Identificados

- Acceso no autorizado a infraestructura crítica.
- Exposición de credenciales de base de datos.
- Posible pérdida o alteración de información.
- Riesgo reputacional.
- Interrupción de servicios (DoS).
- Incumplimiento potencial normativo.

Nivel de Riesgo Antes del Hardening
CRÍTICO

Nivel de Riesgo Después del Hardening
MEDIO-BAJO (técnico)
MEDIO (organizativo)

3. Causa Raíz

El incidente no fue producto de una vulnerabilidad zero-day, sino de:

- Falta de gobierno formal de seguridad.
- Configuraciones por defecto inseguras.
- Gestión débil de credenciales.
- Ausencia de monitoreo continuo.
- No existencia de análisis de riesgos documentado.

El modelo de seguridad era reactivo y no preventivo.

4. Acciones Correctivas Ejecutadas

Medidas Técnicas Implementadas

- Deshabilitación completa de FTP (puerto 21 cerrado).
- Eliminación de PermitRootLogin.
- Autenticación SSH únicamente por clave pública.
- Cambio total de credenciales.
- Restricción de MySQL a localhost.
- Permisos restrictivos en wp-config.php.
- Actualización y limpieza del sistema.
- Configuración de controles anti-DoS.

Resultado: reducción significativa de superficie de ataque.

5. Evaluación de Madurez de Seguridad

Dimensión	Antes	Después
Gobierno de Seguridad	Inexistente	Básico
Gestión de Riesgos	Reactiva	Formalizable
Controles Técnicos	Críticamente débiles	Endurecidos
Monitorización	Nula	Básica
Cumplimiento Normativo	Bajo	Medio

Madurez global estimada: **Nivel 2 – Risk Informed (NIST)**

6. Situación de Cumplimiento

ISO 27001

- No certificable actualmente.

- Falta política formal.
- No existe SoA.
- No hay auditoría interna documentada.

NIST CSF

Cobertura parcial en funciones Protect, Respond y Recover.
Débil en Identify y Detect.

ENS (Nivel Medio estimado)

Cumplimiento técnico parcial, pero insuficiente a nivel organizativo.

7. Recomendaciones Estratégicas para Dirección

Fase 1 – Formalización (0–3 meses)

- Aprobar Política Corporativa de Seguridad.
- Elaborar Análisis Formal de Riesgos (ISO 27005).
- Definir responsables y segregación de funciones.
- Clasificación oficial del sistema (ENS).

Fase 2 – Controles Avanzados (3–6 meses)

- Implementar SIEM (Wazuh / Elastic).
- Implementar Fail2Ban permanente.
- Implementar WAF.
- MFA obligatorio en accesos administrativos.
- Monitorización continua de logs.

Fase 3 – Cumplimiento (6–12 meses)

- Elaborar Statement of Applicability.
- Auditoría interna anual.
- Procedimiento formal de gestión de incidentes.

- Preparación para certificación ISO 27001.

8. Conclusión para Gerencia

El incidente evidenció una **debilidad estructural en el gobierno de seguridad**, no únicamente un fallo técnico.

La infraestructura actualmente se encuentra técnicamente protegida, pero:

- No existe aún un Sistema de Gestión de Seguridad formal.
- El cumplimiento es técnico, no organizativo.
- La organización es vulnerable a nuevos incidentes si no evoluciona hacia un modelo preventivo.

El hardening ejecutado permite ahora iniciar un proceso serio de madurez y certificación.

9. Decisión Estratégica Recomendada

La dirección debe definir si:

A) Se mantiene un enfoque reactivo mínimo.
B) Se invierte en un modelo estructurado alineado con ISO 27001 y ENS.

Recomendación del consultor:
Adoptar modelo B para reducir riesgo reputacional, operativo y legal a medio plazo.

Si lo deseas, puedo prepararte:

- Versión reducida de 1 página para comité.
- Versión tipo PowerPoint ejecutiva.
- Versión orientada a auditoría externa.
- Resumen para Consejo de Administración.
- Documento listo para impresión con formato corporativo.

10. Impacto Económico Potencial de No Actuar

No corregir estructuralmente las debilidades detectadas puede generar impactos financieros significativos en múltiples dimensiones:

10.1 Pérdidas por Interrupción Operativa (Downtime)

Un ataque exitoso (DoS, ransomware, exfiltración o toma de control) podría provocar:

- Caída del sitio web corporativo.
- Interrupción de servicios al cliente.
- Paralización de operaciones internas.

Impacto estimado:

- Pérdida directa de ingresos por hora de inactividad.
- Costes de recuperación técnica urgente.
- Penalizaciones contractuales por incumplimiento de SLA.
- Costes extraordinarios de soporte externo.

En empresas digitales, una interrupción de 24–72 horas puede representar **pérdidas de miles o decenas de miles de euros**, dependiendo del volumen de negocio.

10.2 Impacto Reputacional

Una filtración de credenciales o compromiso público puede generar:

- Pérdida de confianza de clientes.
- Deterioro de imagen de marca.
- Cancelación de contratos.
- Dificultad en captación de nuevos clientes.

El daño reputacional suele ser más costoso que el incidente técnico en sí, ya que afecta al valor intangible de la marca.

10.3 Riesgo Legal y Sancionador

Si existiera exposición de datos personales o información sensible, podrían activarse obligaciones regulatorias bajo:

- Agencia Española de Protección de Datos
- Normativa ENS (si aplica sector público).
- Requisitos contractuales de seguridad.

Las sanciones por incumplimiento en materia de protección de datos pueden alcanzar **hasta el 4% de la facturación anual global**, dependiendo de la gravedad y negligencia demostrada.

Además, podrían existir:

- Demandas civiles.
- Reclamaciones por daños.
- Costes legales y periciales.

10.4 Coste de Respuesta Reactiva vs. Prevención

Existe una diferencia crítica entre:

- Inversión preventiva estructurada (políticas, SIEM, MFA, hardening continuo).
- Respuesta reactiva tras incidente grave.

Estudios internacionales alineados con marcos como los del National Institute of Standards and Technology demuestran que:

> El coste de recuperación tras incidente puede ser entre 5 y 10 veces superior al coste de prevención.

Costes típicos post-incidente:

- Forense externo especializado.
- Restauración desde backups.
- Reconfiguración total de infraestructura.
- Auditoría legal.
- Comunicación de crisis.
- Monitorización de identidad para clientes afectados.

10.5 Riesgo Estratégico a Medio Plazo

Ignorar estas vulnerabilidades puede implicar:

- Exclusión en licitaciones públicas (requisitos ENS).
- Imposibilidad de certificación ISO 27001.
- Dificultad para firmar contratos con clientes enterprise.
- Pérdida de ventaja competitiva.

La seguridad ya no es solo un requisito técnico; es un habilitador comercial.

10.6 Estimación de Escenario de Peor Caso

En un escenario crítico (brecha pública + caída de servicio + sanción):

- Recuperación técnica: 10.000 – 40.000 €
- Impacto reputacional indirecto: difícilmente cuantificable
- Posible sanción regulatoria: variable según facturación
- Pérdida de contratos: potencialmente superior al coste técnico

El impacto total podría superar ampliamente el coste de implementar un programa estructurado de seguridad.

11. Conclusión Económica para Dirección

No actuar no implica “ahorro”, sino **traslado del coste al futuro con multiplicador de riesgo**.

La inversión en:

- Gobierno de seguridad
- Monitorización continua
- Gestión formal de riesgos
- Cumplimiento normativo

debe considerarse una **inversión en protección de activos, continuidad de negocio y reputación corporativa**, no un gasto técnico.