
INFORME DE PRUEBAS DE INTRUSIÓN (PENTESTING)

ECOticias, S.L.

Evaluación de Seguridad Técnica – Informe Final
Fecha: 28/05/2026
Elaborado por: Departamento de Ciberseguridad

---

1. Resumen Ejecutivo

El presente informe recoge los resultados de las pruebas de intrusión realizadas sobre la infraestructura tecnológica de **ECOticias, S.L.** con el objetivo de identificar vulnerabilidades explotables, evaluar el nivel de exposición ante amenazas reales y determinar el grado de madurez en materia de ciberseguridad.

Las pruebas se realizaron siguiendo metodologías reconocidas (PTES, OWASP, MITRE ATT&CK) y se centraron en los sistemas críticos definidos en el alcance.

Los resultados muestran vulnerabilidades de severidad **alta**, **media** y **baja**, algunas de ellas explotables de forma remota sin autenticación.

Conclusión general:
El riesgo global se considera **alto**, especialmente debido a la presencia de una vulnerabilidad crítica en el portal web y a configuraciones débiles en accesos remotos.

---

2. Alcance del Proyecto

2.1 Sistemas incluidos

- Portal web corporativo: www.ecoticias.es
- Servidor de correo electrónico
- Plataforma VPN de acceso remoto
- Aplicación interna de gestión documental
- Estaciones de trabajo representativas

2.2 Tipología de pruebas

- Pentesting externo (caja negra)
- Pentesting interno (caja gris)

- Análisis de vulnerabilidades
- Revisión de configuraciones
- Pruebas de explotación controlada

2.3 Exclusiones

- Sistemas industriales o SCADA
- Infraestructura cloud gestionada por terceros

---

3. Metodología Aplicada

La ejecución del proyecto siguió el estándar **PTES**, estructurado en las siguientes fases:

1. Reconocimiento pasivo
2. Enumeración activa
3. Identificación de vectores de ataque
4. Análisis de vulnerabilidades
5. Explotación
6. Escalada de privilegios
7. Post-explotación
8. Documentación y recomendaciones

Todas las acciones se realizaron de forma controlada, sin afectar a la disponibilidad de los servicios.

---

4. Resultados del Análisis

4.1 Vulnerabilidades Críticas

VUL-001 – Inyección SQL en el portal web

- **Severidad:** Alta
- **Descripción:** El parámetro id del módulo de noticias permite inyección SQL.
- **Impacto:** Acceso completo a la base de datos, extracción de información sensible y potencial ejecución de comandos.

- **Evidencia:**
    - Payload: ' OR 1=1--
    - Respuesta: listado completo de registros sin filtrado.
- **Riesgo:** Compromiso total del backend.
- **Recomendación:** Uso de consultas preparadas, validación estricta y despliegue de WAF.

4.2 Vulnerabilidades de Severidad Media

VUL-010 – Contraseñas débiles en VPN

- **Severidad:** Media
- **Descripción:** Se identificaron credenciales vulnerables mediante ataques de diccionario.
- **Impacto:** Acceso no autorizado a la red interna.
- **Recomendación:** Políticas de contraseñas robustas y activación de MFA.

VUL-014 – Servidor web con versión obsoleta

- **Severidad:** Media
- **Descripción:** Apache ejecuta una versión afectada por vulnerabilidades conocidas (CVE-2023-25690).
- **Recomendación:** Actualización inmediata y endurecimiento de configuración.

4.3 Vulnerabilidades de Severidad Baja

VUL-021 – Ausencia de cabeceras de seguridad

- **Severidad:** Baja
- **Descripción:** Faltan cabeceras como CSP, X-Frame-Options y X-XSS-Protection.
- **Impacto:** Mayor exposición a ataques XSS y clickjacking.
- **Recomendación:** Configurar cabeceras de seguridad estándar.

---

5. Pruebas de Explotación

Durante la fase de explotación se consiguió:

- Acceso a la base de datos del portal web.
- Enumeración de usuarios internos.
- Acceso parcial a la red mediante credenciales débiles.
- Escalada de privilegios en un equipo Windows mediante vulnerabilidad local.

No se realizaron modificaciones ni acciones destructivas.

---

6. Evaluación del Riesgo Global

Categoría	**Nivel**
Riesgo técnico	**Alto**
Riesgo operativo	**Medio**
Riesgo reputacional	**Medio-Alto**
Riesgo de cumplimiento	**Medio**

---

7. Recomendaciones Prioritarias

1. Corrección inmediata de la inyección SQL.
2. Actualización de servidores y aplicación de parches.
3. Activación de MFA en todos los accesos remotos.
4. Revisión de políticas de contraseñas y rotación.
5. Implementación de WAF y mejora de la monitorización.
6. Realización de auditorías periódicas y pentesting anual.

---

8. Conclusiones

ECOticias, S.L. presenta un nivel de riesgo elevado debido a vulnerabilidades críticas explotables desde Internet. La aplicación de las medidas recomendadas reducirá significativamente la superficie de ataque y mejorará la resiliencia del entorno.

El equipo de ciberseguridad queda disponible para acompañar en la fase de remediación y validación posterior.

---

9. Anexos

- Evidencias técnicas
- Capturas de tráfico
- Hashes de pruebas
- Listado de CVEs
- Cronograma de actividades

¿Quieres que te genere también la portada corporativa, la tabla de contenidos automática o el diseño con estilos de Word (H1, H2, H3) para que el documento quede totalmente profesional?