# \*\*(1) Resumen Ejecutivo\*\*

El proveedor presenta múltiples hallazgos de riesgo en su infraestructura y prácticas de gestión de datos. Se identifican vulnerabilidades como dominios phishing, exposición de puertos con credenciales débiles, filtración de datos, certificados TLS caducados y sanciones anteriores por incumplimiento de RGPD. Aunque participa en programas de Bug Bounty, la falta de controles como SBOM, trazabilidad de accesos y gestión de vulnerabilidades recurrente eleva el riesgo. El cumplimiento parcial de requisitos de seguridad y protección de datos, junto con la exposición de backups, sugiere una falta de madurez en su modelo de seguridad.

# \*\*(2) Nivel de Riesgo General: ALTO (85%)\*\*

\*\*Justificación\*\*:

- \*\*Riesgo de exposición de datos\*\*: Hallazgos como el filtrado de hashes de contraseñas y directorios de backup accesibles (OSINT) indican falta de protección de información sensibles, compatible con RGPD y NIS2.

- \*\*Falta de controles críticos\*\*: Ausencia de SBOM, trazabilidad de accesos (RS-CB-04), y gestión de vulnerabilidades recurrente (RS-CB-02) viola ISO 27001:2022 y DORA.

- \*\*Incumplimiento normativo\*\*: Sanción de AEPD por uso inadecuado de datos personales y certificados TLS caducados (OSINT) ponen en riesgo el cumplimiento de RGPD y ENS.

- \*\*Vulnerabilidades explotables\*\*: Puertos expuestos con credenciales débiles (Shodan) y phishing (VirusTotal) aumentan la exposición a ataques externos.

# \*\*(3) Controles Críticos No Cumplidos o Parcialmente Cumplidos\*\*

1. \*\*Falta de SBOM (RS-SD-05)\*\*: No disponible para garantizar transparencia en dependencias de software, violando ISO 27001:2022 y DORA.

2. \*\*Gestión de vulnerabilidades inadecuada (RS-CB-02)\*\*: Escaneo no recurrente y sin plan de resolución, lo que exponen a riesgos de ataques.

3. \*\*Trazabilidad de accesos y logs (RS-CB-04)\*\*: Ausencia de monitoreo, facilitando el acceso no autorizado y dificultando la auditoría.

4. \*\*Anonimización parcial de datos (RS-SD-06)\*\*: Solo en algunos proyectos, lo que no cumple con RGPD y ENS.

5. \*\*Certificados TLS caducados y gestionados de forma inadecuada (OSINT)\*\*: Vulneran la seguridad de comunicaciones, contraviniendo ENS y NIS2.

---

# \*\*(4) Recomendaciones Específicas y Priorizadas\*\*

1. \*\*Implementar SBOM y gestión de vulnerabilidades recurrente\*\*: Crear un plan de resolución de vulnerabilidades con escaneo mensual y actualización de dependencias (ISO 27001:2022, DORA).

2. \*\*Revisar y actualizar certificados TLS\*\*: Corregir certificados caducados y garantizar validación de subdominios críticos (RGPD, NIS2).

3. \*\*Establecer trazabilidad de accesos y logs automatizados\*\*: Integrar SIEM para monitoreo en tiempo real y cumplir con RS-CB-04 y RS-CB-05 (ISO 27001:2022).

---

# \*\*(5) Conclusión\*\*

El proveedor requiere mejoras urgentes en controles de seguridad y cumplimiento normativo para mitigar riesgos.

---

\*Nota: El informe se basa únicamente en los datos proporcionados y no incluye información externa.\*