# Informe de Auditoría de Ciberseguridad y Cumplimiento Normativo - Requisitos Software

## 1. Resumen Ejecutivo

El presente informe analiza el nivel de madurez en ciberseguridad y cumplimiento normativo de proveedor-soft.com, a partir de hallazgos OSINT y de las respuestas al cuestionario Requisitos Software. Se identifican incidentes previos de seguridad relevantes, como exposición de servicios críticos, filtraciones de credenciales, caducidad de certificados TLS, publicación indebida de documentación técnica y sanciones regulatorias. Aunque la empresa participa en programas de Bug Bounty y ha mostrado avances en la corrección de vulnerabilidades, persisten carencias significativas en gestión de accesos, protección de datos, trazabilidad de eventos, seguridad en el desarrollo de software e integración de medidas específicas para el uso de inteligencia artificial. Estas debilidades comprometen el cumplimiento de marcos como ENS, ISO 27001:2022, RGPD, NIS2, DORA y CRA. El riesgo general se considera alto.

## 2. Nivel de Riesgo General

Nivel de riesgo: ALTO (80%)

Justificación: El proveedor presenta deficiencias críticas en seguridad de software: ausencia de SBOM, gestión ineficaz de accesos y privilegios, falta de cifrado completo, deficiencias en pruebas de seguridad, localización de datos fuera de la UE y debilidades en el uso de IA. Aunque existen medidas parciales (segregación de entornos, cifrado en tránsito, integración SAML2, programas Bug Bounty), el nivel de exposición frente a amenazas y sanciones regulatorias sigue siendo elevado.

## 3. Controles Críticos No Cumplidos o Parcialmente Cumplidos

- RS-SD-04: No existe revisión anual de privilegios de desarrolladores.

- RS-SD-05: No se dispone de Software Bill of Materials (SBOM).

- RS-CB-04: No existe trazabilidad de accesos ni logs adecuados.

- RS-DA-01/RS-DA-04: No se aplica cifrado integral ni segregación de datos por cliente.

- RS-GI-03: Ausencia de controles avanzados de seguridad en software (WAF, DLP, CASB).

- RS-SN-02: Centros de datos fuera de la UE, incumpliendo requisitos de localización.

- RS-IA-06/RS-IA-08/RS-IA-09: Carencia de controles frente a filtración de datos, evaluación regulatoria y certificaciones en IA.

## 4. Recomendaciones Específicas y Priorizadas

1. Implementar de forma prioritaria una revisión periódica de accesos y privilegios, con segregación de funciones.

2. Adoptar un SBOM actualizado y escaneos recurrentes de vulnerabilidades, con planes de remediación verificables.

3. Fortalecer los controles de trazabilidad y centralización de logs, con integración automática en un SIEM.

4. Aplicar cifrado completo en tránsito, uso y almacenamiento, con segregación de datos por cliente conforme a RGPD y CRA.

5. Desplegar controles avanzados de seguridad (WAF, DLP, CASB) para proteger aplicaciones críticas.

6. Revisar la estrategia de IA, aplicando mecanismos de protección frente a fugas de datos, parches automáticos y evaluaciones de cumplimiento normativo en línea con ISO 42001.

7. Reubicar o garantizar adecuación legal de los centros de datos fuera de la UE para cumplir con RGPD y NIS2.

## 5. Conclusión

Proveedor-soft.com presenta un nivel de riesgo alto, requiriendo acciones inmediatas en seguridad de software, protección de datos y cumplimiento regulatorio para garantizar confianza y continuidad en sus servicios.