# \*\*1. Resumen Ejecutivo\*\*

En este informe se analizan los hallazgos obtenidos mediante OSINT y las respuestas a un cuestionario de requisitos de software de la empresa proveedor-soft.com. Se identifican factores que elevan el riesgo de ciberseguridad y no cumplimiento con normas regulatorias.

# \*\*2. Nivel de Riesgo General\*\*

El nivel de riesgo general es \*\*ALTO (80-100%)\*\* debido a la exposición de URL phishing, credenciales débiles, publicación de hashes de contraseñas, accesibilidad de directorios de backup y certificado TLS caducado. Además, existen indicaciones de falta de control en accesos a entornos de desarrollo y sanciones por uso inadecuado de datos personales.

# \*\*3. Controles Críticos No Cumplidos o Parcialmente Cumplidos\*\*

a) Revisión Anual de Privilegios de Desarrolladores (No cumplido)

b) SBOM Disponible (No cumplido)

c) Anonimización de Datos en Preproducción (Parcial)

d) Escaneo de Vulnerabilidades y Plan de Resolución (Parcial, no recurrente)

e) Trazabilidad de Accesos y Logs (No cumplido)

# \*\*4. Recomendaciones Específicas y Priorizadas\*\*

a) Realizar una revisión anual de privilegios de desarrolladores y establecer un procedimiento formalizado para garantizar el control de acceso en los entornos de desarrollo.

b) Crear y mantener un Software Bill of Materials (SBOM) para brindar transparencia sobre los componentes del software.

c) Establecer un plan de escaneo de vulnerabilidades y resolución recurrente, así como un sistema de trazabilidad de accesos y logs.

# \*\*5. Conclusión\*\*

La empresa proveedor-soft.com debe priorizar la mejora de su ciberseguridad y compliancia regulatoria. Los controles críticos no cumplidos y parcialmente cumplidos identificados en el informe deben ser abordados de inmediato para reducir el riesgo general y asegurar la confianza de sus clientes.