# \*\*Resumen Ejecutivo:\*\*

El proveedor-soft.com presenta varios hallazgos de seguridad potenciales identificados mediante investigación OSINT y respuestas al Anexo II. Se han detectado dos url marcadas como phishing en VirusTotal en 2024, credenciales débiles en Shodan en 2023, públicación de usuarios y hashes de contraseñas, accesibles directorios de backup, certificado TLS caducado, sanciones por uso inadecuado de datos personales, y falta de control en accesos a entornos de desarrollo. Aunque participa en programas de Bug Bounty y publica reportes de vulnerabilidades corregidas, carece de ciertos controles críticos.

# \*\*Nivel de Riesgo General:\*\*

El nivel de riesgo general para el proveedor-soft.com se evalúa en ALTO. Las vulnerabilidades identificadas en la investigación OSINT y las respuestas al Anexo II pueden resultar en pérdida de datos, pérdida de funcionalidad, daño a la reputación, o sanciones regulatorias. El porcentaje de riesgo se estimaba en un 85%.

# \*\*Controles Críticos No Cumplidos o Parcialmente Cumplidos:\*\*

1. Revisión Anual de Privilegios de Desarrolladores (RS-SD-04): El proveedor no realiza revisiones anuales de privilegios de desarrolladores.

2. Anonimización de Datos en Preproducción (RS-SD-06): Solo algunos proyectos de la empresa anonimizan datos en preproducción.

3. Trazabilidad de Accesos y Logs (RS-CB-04): El proveedor no registra logs de accesos.

# \*\*Recomendaciones Específicas y Priorizadas:\*\*

1. El proveedor debe implementar una política de revisión anual de privilegios de desarrolladores.

2. La empresa debe anonimizar todos los datos en preproducción.

3. El proveedor debe implementar un sistema de logs de accesos y trazar los mismos.

# \*\*Conclusión:\*\*

El proveedor-soft.com presenta un nivel de riesgo alto debido a varias vulnerabilidades identificadas en la investigación OSINT y las respuestas al Anexo II. Para reducir este riesgo, se recomienda la implementación de controles críticos como la revisión anual de privilegios de desarrolladores, la anonimización de todos los datos en preproducción, y el registro de logs de accesos.