En este informe, se presentan los hallazgos de una evaluación OSINT y las respuestas del proveedor al cuestionario del Anexo II del Requisito Software. Los hallazgos indican una serie de vulnerabilidades y riesgos cibernéticos, incluyendo exposiciones de credenciales débiles, directorios de backup accesibles y un certificado TLS caducado. A pesar de la participación del proveedor en programas de Bug Bounty y la publicación de reportes de vulnerabilidades corregidas, se identifican controles críticos no cumplidos o parcialmente cumplidos. En este informe, se presentan las conclusiones y recomendaciones específicas y priorizadas para mejorar la ciberseguridad y el cumplimiento normativo del proveedor.

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

El nivel de riesgo general es MEDIUM (50-75%) debido a la combinación de vulnerabilidades y controles críticos no cumplidos o parcialmente cumplidos.

# \*\*Controles Críticos no Cumplidos o Parcialmente Cumplidos\*\*

1. \*\*Revisión anual de privilegios de desarrolladores\*\*: No cumple con el requisito de revisión anual de privilegios de desarrolladores.

2. \*\*Anonimización de datos en preproducción\*\*: Solo es parcial y no cubre todos los proyectos.

3. \*\*Protección frente a DoS\*\*: Aunque se cumple con el requisito básico, no se proporciona información adicional sobre la implementación.

4. \*\*Trazabilidad de accesos y logs\*\*: No cumple con el requisito de trazabilidad de accesos y logs.

5. \*\*Entrega de logs a SIEM/API\*\*: Solo es parcial y no se proporciona información adicional sobre la implementación.

6. \*\*Cifrado en tránsito, uso y almacenamiento\*\*: Solo es parcial y no cubre todos los casos.

7. \*\*Limitación de funcionalidades de IA\*\*: No cumple con el requisito de limitación de funcionalidades de IA.

8. \*\*Filtrado y saneamiento de datos externos en IA\*\*: No cumple con el requisito de filtrado y saneamiento de datos externos en IA.

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

1. \*\*Implementar revisión anual de privilegios de desarrolladores\*\*: Para garantizar la seguridad de los sistemas y la protección de datos.

2. \*\*Aumentar la anonimización de datos en preproducción\*\*: Para proteger los datos de los usuarios y cumplir con el requisito de anonimización.

3. \*\*Implementar trazabilidad de accesos y logs\*\*: Para garantizar la seguridad y la transparencia en la gestión de accesos a los sistemas.

4. \*\*Aumentar la entrega de logs a SIEM/API\*\*: Para mejorar la seguridad y la respuesta a incidentes cibernéticos.

5. \*\*Implementar cifrado en tránsito, uso y almacenamiento\*\*: Para proteger los datos de los usuarios y cumplir con el requisito de cifrado.

# \*\*Conclusión\*\*

La evaluación de ciberseguridad y cumplimiento normativo ha identificado una serie de vulnerabilidades y controles críticos no cumplidos o parcialmente cumplidos. Se recomienda implementar controles adicionales para garantizar la seguridad de los sistemas y la protección de datos.