# \*\*Resumen Ejecutivo\*\*

La empresa "Proveedor" ha sido objeto de análisis OSINT y evaluación de respuestas a un cuestionario de cumplimiento normativo. Los hallazgos OSINT han revelado varias vulnerabilidades y riesgos en la seguridad de la información y el cumplimiento normativo. A pesar de que la empresa participa en programas de Bug Bounty y publica reportes de vulnerabilidades corregidas, los hallazgos indican una falta de cumplimiento normativo en varios aspectos.

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

El nivel de riesgo general de la empresa es MEDIO (50%). La empresa tiene una falta de cumplimiento normativo en varios aspectos, lo que puede exponerla a riesgos de seguridad y cumplimiento normativo.

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

1. \*\*RS-SD-04: Revisión anual de privilegios de desarrolladores\*\*: No se ha realizado una revisión anual de los privilegios de los desarrolladores, lo que puede exponer a la empresa a riesgos de seguridad.

2. \*\*RS-CB-04: Trazabilidad de accesos y logs\*\*: No se tiene trazabilidad de los accesos y logs, lo que puede dificultar la detección de incidentes de seguridad.

3. \*\*RS-DA-03: Estrategia de seguridad de comunicaciones\*\*: No se tiene una estrategia de seguridad de comunicaciones, lo que puede exponer a la empresa a riesgos de seguridad en la transmisión de datos.

4. \*\*RS-SN-02: Ubicación UE de data centers\*\*: Los data centers no están ubicados en la Unión Europea, lo que puede afectar al cumplimiento normativo en relación con la protección de datos.

5. \*\*RS-IA-08: Evaluación de cumplimiento regulatorio en IA\*\*: No se evalúa el cumplimiento regulatorio en relación con la inteligencia artificial (IA), lo que puede exponer a la empresa a riesgos de cumplimiento normativo.

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

1. \*\*Realizar una revisión anual de privilegios de desarrolladores\*\*: La empresa debe realizar una revisión anual de los privilegios de los desarrolladores para asegurarse de que no haya acceso no autorizado a la información confidencial.

2. \*\*Implementar trazabilidad de accesos y logs\*\*: La empresa debe implementar trazabilidad de los accesos y logs para facilitar la detección de incidentes de seguridad.

3. \*\*Desarrollar una estrategia de seguridad de comunicaciones\*\*: La empresa debe desarrollar una estrategia de seguridad de comunicaciones para asegurarse de que la transmisión de datos esté protegida.

# \*\*Conclusión\*\*

La empresa "Proveedor" tiene una falta de cumplimiento normativo en varios aspectos, lo que puede exponerla a riesgos de seguridad y cumplimiento normativo. Es recomendable que la empresa tome medidas para remediar estas vulnerabilidades y asegurese de que cumpla con los requisitos de seguridad y cumplimiento normativo.