# \*Informe Técnico de Cumplimiento Normativo y Ciberseguridad\*\*

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

El proveedor presenta múltiples brechas en su postura de seguridad, incluyendo cuatro filtraciones de datos en dos años, exposición de puertos sin autenticación, documentos confidenciales indexados en Google, y archivos sospechosos en VirusTotal. Aunque existen políticas documentadas, el cumplimiento normativo es parcial o inexistente, sin certificaciones reconocidas (ENS, ISO 27001, etc.). Falta de controles críticos como MFA, cifrado de discos, auditoría de terceros y plan de continuidad de negocio eleva significativamente el riesgo. La ausencia de un responsable formal de seguridad y mecanismos de notificación de incidentes agrega vulnerabilidad.

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

\*\*ALTO (85%)\*\*

Justificación: El historial de filtraciones (1), exposición de puertos vulnerables (2), documentos confidenciales indexados (3) y archivos sospechosos (4) indican una infraestructura con riesgos críticos. La falta de certificaciones (5), controles de acceso fuerte (6) y plan de continuidad (7) intensifica la exposición a ataques. Aunque no se reportan incidentes recientes (6), la presencia de accesos no autorizados en 2023 y la ausencia de auditorías de terceros mantienen el riesgo en niveles altos.

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

1. \*\*Ausencia de responsable formal de seguridad\*\* (no respondido).

2. \*\*Ubicación geográfica imprecisa\*\* de tratamiento de datos (parcial).

3. \*\*Falta de análisis de riesgos específicos\*\* para contratos (no).

4. \*\*No certificaciones reconocidas\*\* (ENS, ISO 27001, etc.) (no).

5. \*\*Procesos de destrucción segura de información\*\* sin respaldo técnico (no).

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

1. \*\*Implementar certificaciones ISO 27001 o ENS\*\* y documentar cumplimiento normativo (RGPD, NIS2, DORA) para validar procesos.

2. \*\*Establecer MFA, control de accesos lógicos y auditoría de terceros\*\*, incluyendo verificación de subcontratistas.

3. \*\*Definir un plan de continuidad de negocio con RTO/RPO\*\* y mecanismos de notificación formal de incidentes.

# \*\*5. Conclusión\*\*

El proveedor enfrenta riesgos altos debido a brechas en seguridad, cumplimiento normativo y controles críticos. Es urgente adoptar medidas de certificación, accesos restringidos y planificación de continuidad.