# \*\*Informe Técnico de Auditoría de Ciberseguridad y Compliance Normativo\*\*

# \*\*Resumen Ejecutivo\*\*

En esta evaluación de ciberseguridad y compliancia normativa, se ha detectado un nivel alto de riesgo general en el proveedor-test.com. El proveedor ha demostrado cierta capacidad en el manejo de roles y responsabilidades de seguridad, así como la existencia de políticas internas de seguridad documentadas. Sin embargo, carece de un marco de trabajo efectivo en varios aspectos clave, como la falta de un responsable formal de seguridad, la ubicación imprecisa de su centro de datos y la ausencia de contratos específicos con sus proveedores de servicios.

# \*\*Nivel de riesgo general (ALTO)\*\*

El nivel de riesgo general se evalúa como alto (90%). La evidencia de filtraciones de datos, accesos no autorizados, pruebas de antivirus fallidas y la ausencia de contratos específicos con sus proveedores de servicios representan un riesgo considerable para la privacidad y la integridad de los datos de los clientes.

# \*\*Controles críticos no cumplidos o parcialmente cumplidos\*\*

1. \*\*No se ha designado un responsable formal de seguridad con datos de contacto\*\*

2. \*\*La ubicación del tratamiento de la información se describe sin precisión geográfica\*\*

3. \*\*No ha realizado un análisis de riesgos específico para el contrato\*\*

4. \*\*No aporta documentación técnica sobre la arquitectura del servicio\*\*

5. \*\*No verifica ni audita a los terceros subcontratados\*\*

6. \*\*No contempla cómo notificar incidentes ni colaborar formalmente con el cliente\*\*

7. \*\*No dispone de ninguna certificación reconocida ni evidencia documental de cumplimiento normativo\*\*

# \*\*Recomendaciones específicas y priorizadas\*\*

1. \*\*Designar un responsable formal de seguridad con datos de contacto\*\*

2. \*\*Realizar un análisis de riesgos específico para el contrato y documentarlo\*\*

3. \*\*Adoptar contratos específicos con terceros subcontratados que garantice la seguridad\*\*

4. \*\*Implementar medidas de seguridad efectivas en la arquitectura del servicio\*\*

5. \*\*Aplicar MFA y control de accesos lógico o físico\*\*

6. \*\*Monitorear eventos de seguridad y revisar los accesos\*\*

7. \*\*Fomentar la formación continua en ciberseguridad para el personal\*\*

# \*\*Conclusión\*\*

Se recomienda al proveedor-test.com que adopte medidas efectivas en ciberseguridad y cumplimiento normativo para proteger mejor la privacidad y la integridad de los datos de los clientes. La carencia de contratos específicos con terceros subcontratados y la ausencia de análisis de riesgos específicos para el contrato constituyen puntos críticos que deben ser resueltos de inmediato.