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

\*\*Resumen Ejecutivo\*\*

Se ha llevado a cabo una evaluación de ciberseguridad y cumplimiento normativo en el proveedor "test.com" con el fin de determinar el nivel de riesgo y cumplimiento con los marcos de referencia ENS, ISO 27001:2022, RGPD, NIS2 y DORA. Los hallazgos OSINT han revelado varias vulnerabilidades y debilidades, incluyendo filtraciones de datos, exposición de puertos sin autenticación, indexación de documentos confidenciales y accesos no autorizados. A pesar de que el proveedor ha implementado algunas medidas de seguridad, se han identificado controles críticos no cumplidos o parcialmente cumplidos.

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

El nivel de riesgo general se clasifica como \*\*ALTO\*\* (80%). Esto se debe a la combinación de hallazgos OSINT y respuestas del proveedor que indican una falta de cumplimiento con los marcos de referencia mencionados. Las principales áreas de riesgo son la seguridad de la información, la privacidad y la protección contra ciberataques.

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

1. \*\*Análisis de Riesgos\*\*: El proveedor no ha realizado un análisis de riesgos específico para el contrato, lo que hace imposible determinar la probabilidad y el impacto de los riesgos.

2. \*\*Seguridad de la Información\*\*: El proveedor no tiene un inventario técnico ni políticas de actualización, lo que pone en riesgo la seguridad de la información.

3. \*\*Acceso Remoto\*\*: El acceso remoto no está restringido ni protegido por autenticación fuerte, lo que permite accesos no autorizados.

4. \*\*Cifrado de Datos\*\*: El proveedor no cifra los discos ni bloquea dispositivos externos, lo que expone la información a riesgos de acceso no autorizado.

5. \*\*Monitoreo de Seguridad\*\*: El proveedor no revisa los accesos ni monitoriza eventos de seguridad, lo que hace difícil detectar incidentes de seguridad.

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

1. \*\*Realizar un Análisis de Riesgos\*\*: El proveedor debe realizar un análisis de riesgos específico para el contrato para determinar la probabilidad y el impacto de los riesgos.

2. \*\*Implementar Medidas de Seguridad\*\*: El proveedor debe implementar medidas de seguridad, incluyendo cifrado de datos, bloqueo de dispositivos externos y autenticación fuerte para el acceso remoto.

3. \*\*Revisar y Actualizar Políticas\*\*: El proveedor debe revisar y actualizar sus políticas de seguridad para garantizar que estén alineadas con los marcos de referencia mencionados.

\*\*Conclusión\*\*

El proveedor "test.com" enfrenta un alto nivel de riesgo de ciberseguridad y cumplimiento normativo. Es fundamental que el proveedor implemente las recomendaciones mencionadas para mitigar los riesgos y garantizar la seguridad de la información.