# Informe Técnico de Ciberseguridad y Cumplimiento Normativo

## Resumen Ejecutivo

El proveedor-test.com ha demostrado una serie de vulnerabilidades y carencias en su implementación de ciberseguridad y cumplimiento normativo. Aunque existen algunos controles básicos, como la clasificación de la información y la etiquetado de los documentos, la falta de transparencia y documentación técnica sobre la arquitectura del servicio, la ausencia de certificaciones reconocidas y la falta de medidas de seguridad física y de continuidad de negocio son preocupantes. Este informe identifica los hallazgos OSINT y las respuestas del proveedor, y presenta una evaluación del nivel de riesgo general y recomendaciones específicas para mejorar la seguridad y el cumplimiento normativo.

## Nivel de Riesgo General

El nivel de riesgo general es alto, con un porcentaje del 80% de riesgo, debido a la combinación de vulnerabilidades y carencias en la implementación de ciberseguridad y cumplimiento normativo**.** La falta de transparencia y documentación técnica sobre la arquitectura del servicio, la ausencia de certificaciones reconocidas y la falta de medidas de seguridad física y de continuidad de negocio aumentan significativamente el riesgo de incidentes y violaciones de datos.

## Controles Críticos No Cumplidos o Parcialmente Cumplidos

1. \*\*Análisis de Riesgos Específico\*\*: El proveedor no ha realizado un análisis de riesgos específico para el contrato, lo que puede llevar a la falta de identificación y mitigación de riesgos potenciales.

2. \*\*Políticas de Manejo de Información\*\*: Las políticas de manejo de información no cuentan con respaldo técnico eficaz, lo que puede afectar la integridad y seguridad de la información.

3. \*\*Procedimiento de Gestión de Incidentes\*\*: El proveedor no contempla cómo notificar los incidentes ni colaborar formalmente con el cliente, lo que puede retrasar la respuesta y mitigación de incidentes.

4. \*\*Certificación de Ciberseguridad\*\*: El proveedor no cuenta con ninguna certificación reconocida, como ENS o ISO 27001, lo que puede afectar la confianza de los clientes y la credibilidad de la empresa.

5. \*\*Mejoras de Seguridad Física\*\*: El proveedor no cuenta con medidas de seguridad física completa, lo que puede comprometer la seguridad de la información y los activos.

## Recomendaciones Específicas y Priorizadas

1. \*\*Realizar un Análisis de Riesgos Específico\*\*: El proveedor debe realizar un análisis de riesgos específico para cada contrato y actualizar las políticas de ciberseguridad y cumplimiento normativo.

2. \*\*Implementar Políticas de Manejo de Información\*\*: El proveedor debe implementar políticas de manejo de información con respaldo técnico eficaz y asegurarse de que se apliquen de manera uniforme.

3. \*\*Definir un Procedimiento de Gestión de Incidentes\*\*: El proveedor debe definir un procedimiento formal para la gestión de incidentes, incluyendo la notificación de incidentes y la colaboración con el cliente.

4. \*\*Obtener Certificación de Ciberseguridad\*\*: El proveedor debe obtener una certificación reconocida de ciberseguridad, como ENS o ISO 27001, para demostrar su compromiso con la seguridad y el cumplimiento normativo.

5. \*\*Implementar Mejoras de Seguridad Física\*\*: El proveedor debe implementar medidas de seguridad física completa, incluyendo la protección de activos y la seguridad de la información.

## Conclusión

El proveedor-test.com debe priorizar la implementación de controles críticos de ciberseguridad y cumplimiento normativo para reducir el riesgo de incidentes y violaciones de datos. Las recomendaciones específicas y priorizadas presentadas en este informe pueden ayudar a mejorar la seguridad y el cumplimiento normativo del proveedor.