# Informe de Auditoría de Ciberseguridad y Cumplimiento Normativo

## 1. Resumen Ejecutivo

El presente informe evalúa la postura de ciberseguridad y cumplimiento normativo del proveedor-test.com, considerando hallazgos OSINT y las respuestas proporcionadas al cuestionario de requisitos generales. Se identifican antecedentes de filtraciones de datos, exposición de servicios críticos sin autenticación, gestión deficiente de la información y ausencia de medidas técnicas y organizativas robustas. Si bien se observa cierta concienciación en su personal y ausencia de incidentes recientes, la organización carece de certificaciones, procesos de análisis de riesgos, controles de acceso efectivos, plan de continuidad de negocio y supervisión de terceros. El nivel de riesgo se considera alto, comprometiendo la confidencialidad, integridad y disponibilidad de los servicios. Se recomienda la adopción inmediata de medidas correctivas priorizadas.

## 2. Nivel de Riesgo General

Nivel de riesgo: ALTO (85%)

Justificación: El proveedor presenta múltiples deficiencias críticas: ausencia de certificaciones reconocidas, falta de análisis de riesgos, no implementación de controles de acceso robustos, carencia de planes de continuidad, deficiente gestión de subcontratación y antecedentes de incidentes de seguridad confirmados en OSINT. Aunque existen elementos positivos (concienciación parcial, etiquetado de información y políticas documentadas), no son suficientes para mitigar los riesgos existentes.

## 3. Controles Críticos No Cumplidos o Parcialmente Cumplidos

- Ausencia de un responsable formal de seguridad con datos de contacto.

- No realización de análisis de riesgos específicos ni definición de RTO/RPO.

- Falta de controles de acceso lógico, MFA y monitorización de eventos.

- No existencia de plan de continuidad de negocio ni pruebas documentadas.

- Subcontratación sin contratos específicos de seguridad ni auditoría de terceros.

- No cifrado de discos ni restricción de dispositivos externos.

- Falta de formación específica en ciberseguridad para el personal.

## 4. Recomendaciones Específicas y Priorizadas

1. Designar formalmente un Responsable de Seguridad con funciones, contacto y autoridad definida.

2. Realizar un análisis de riesgos integral alineado con ENS, ISO 27001, RGPD, NIS2 y DORA, incluyendo definición de RTO/RPO.

3. Implementar controles de acceso avanzados: MFA, registro y monitorización de eventos, restricción de accesos remotos.

4. Establecer un plan de continuidad de negocio con pruebas documentadas y procedimientos de recuperación.

5. Formalizar contratos con subcontratistas que incluyan cláusulas de seguridad, verificaciones y auditorías periódicas.

6. Aplicar cifrado de datos en reposo y en tránsito, así como políticas de uso seguro de dispositivos externos.

7. Desarrollar un programa de formación continua en ciberseguridad para todo el personal técnico y administrativo.

## 5. Conclusión

El proveedor presenta un nivel de riesgo alto y requiere mejoras urgentes en controles técnicos, organizativos y de cumplimiento para garantizar la seguridad y confianza en la prestación de servicios.