Actúas como un auditor experto en ciberseguridad y cumplimiento normativo; tu tarea es generar un informe técnico estructurado a partir de hallazgos OSINT ficticios y de las respuestas de un proveedor al cuestionario del Anexo I (Requisitos Generales), conforme a marcos como ENS, ISO 27001:2022, RGPD, NIS2 y DORA; los hallazgos OSINT son:

(1) el dominio proveedor-test.com ha sufrido cuatro filtraciones de datos en los últimos dos años (HaveIBeenPwned),

(2) la IP 192.0.2.10 tiene el puerto 22 expuesto sin autenticación (Shodan),

(3) un documento PDF confidencial ha sido indexado por Google (Google Dorks), (4) un archivo firmado por proveedor-test.com ha sido marcado como sospechoso por 8 motores antivirus en VirusTotal,

(5) algunos usuarios en foros de ciberseguridad relatan accesos no autorizados vinculados a campañas de phishing en 2023,

(6) sin embargo, no se han detectado nuevos incidentes ni menciones críticas en foros desde hace más de 6 meses,

(7) en redes sociales profesionales se observa que varios perfiles técnicos del proveedor han participado en iniciativas de concienciación sobre ciberseguridad,

(8) los registros de contratación pública muestran contratos adjudicados sin cláusulas explícitas de seguridad, pero sin sanciones ni impugnaciones asociadas;

las respuestas del proveedor son:

1. existencia de roles y responsabilidades de seguridad (sí),
2. no se ha designado responsable formal de seguridad con datos de contacto (no),
3. la ubicación del tratamiento de la información se describe sin precisión geográfica (parcial),
4. dispone de políticas internas de seguridad documentadas (sí),
5. no ha realizado un análisis de riesgos específico para el contrato (no),
6. tiene conocimiento superficial de ENS y RGPD (parcial),
7. no aporta documentación técnica sobre la arquitectura del servicio (no),
8. carece de seguro frente a ciberataques (no),
9. subcontrata sin contratos específicos ni garantías de seguridad (parcial),
10. no verifica ni audita a los terceros subcontratados (no),
11. clasifica la información según sensibilidad (sí),
12. etiqueta los documentos (sí),
13. define controles por clasificación pero no de forma completa ni comprobable (parcial),
14. tiene políticas de manejo de información sin respaldo técnico eficaz (parcial),
15. no cuenta con procesos certificados de destrucción segura (no),
16. dispone de un procedimiento formal para gestionar incidentes (sí),
17. pero no contempla cómo notificarlos ni colaborar formalmente con el cliente (parcial),
18. no dispone de ninguna certificación reconocida (ENS, ISO 27001, etc.) ni evidencia documental de cumplimiento normativo (no),
19. utiliza sus propios equipos para prestar el servicio (sí),
20. no tiene inventario técnico ni políticas de actualización (no),
21. tiene antivirus instalado pero sin validación avanzada (parcial),
22. no cifra los discos ni bloquea dispositivos externos (no),
23. el acceso remoto no está restringido ni protegido por autenticación fuerte (parcial/no),
24. no aplica MFA ni control de accesos lógico o físico (no),
25. no revisa los accesos ni monitoriza eventos de seguridad (no),
26. el personal no recibe formación específica en ciberseguridad (no),
27. dispone de algunas medidas de seguridad física pero sin cobertura completa (parcial),
28. no tiene un plan de continuidad de negocio ni pruebas documentadas (no),
29. y no ha definido RTO/RPO (no);

con toda esta información, genera un informe en español dividido en: (1) resumen ejecutivo (100–150 palabras), (2) nivel de riesgo general (ALTO/MEDIO/BAJO) con justificación y porcentaje del 1% al 100%, (3) controles críticos no cumplidos o parcialmente cumplidos (mínimo cinco), (4) recomendaciones específicas y priorizadas (mínimo tres), (5) conclusión (máximo 50 palabras);

redacta en tono profesional, objetivo y sin añadir información no contenida en el prompt.