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 II (Requisitos Software), conforme a marcos como ENS, ISO 27001:2022, RGPD, NIS2, DORA y CRA;

los hallazgos OSINT son:

(1) el dominio proveedor-soft.com aparece en VirusTotal con dos URL marcadas como phishing en 2024,

(2) Shodan identifica el puerto 3389 expuesto con credenciales débiles en una de sus direcciones IP públicas,

(3) un listado parcial de usuarios y hashes de contraseñas del proveedor fue publicado en un foro clandestino en 2023,

(4) búsquedas avanzadas en Google muestran directorios de backup accesibles con documentación técnica,

(5) un certificado TLS caducado fue detectado en uno de sus subdominios críticos,

(6) la AEPD registra una sanción leve en 2022 por uso inadecuado de datos personales,

(7) en redes sociales técnicas se observan quejas de antiguos empleados sobre falta de control en accesos a entornos de desarrollo,

(8) sin embargo, la empresa participa en programas de Bug Bounty y publica reportes de vulnerabilidades corregidas en los últimos seis meses;

las respuestas del proveedor al Anexo II son:

1. RS-SD-01 desarrollo incluido en contrato (sí),
2. RS-SD-02 metodología de desarrollo seguro (parcial, no formalizada),
3. RS-SD-03 separación de entornos prod/dev (sí),
4. RS-SD-04 revisión anual de privilegios de desarrolladores (no),
5. RS-SD-05 SBOM disponible (no),
6. RS-SD-06 anonimización de datos en preproducción (parcial, solo algunos proyectos),
7. RS-CB-01 provisión de software (sí),
8. RS-CB-02 escaneo de vulnerabilidades y plan de resolución (parcial, no recurrente),
9. RS-CB-03 asunción de resolución de vulnerabilidades (sí),
10. RS-CB-04 trazabilidad de accesos y logs (no),
11. RS-CB-05 entrega de logs a SIEM/API (parcial, manual),
12. RS-CB-06 protección frente a DoS (sí, básica),
13. RS-CB-07 sincronización de relojes (sí, NTP configurado),
14. RS-DA-01 cifrado en tránsito, uso y almacenamiento (parcial, solo en tránsito),
15. RS-DA-02 algoritmos criptográficos (AES-256 en algunos módulos),
16. RS-DA-03 estrategia de seguridad de comunicaciones (no),
17. RS-DA-04 segregación física de datos por cliente (no),
18. RS-GI-01 integración con sistemas de autenticación cliente (sí, SAML2),
19. RS-GI-02 aplicación de mínimo privilegio (parcial),
20. RS-GI-03 controles avanzados de seguridad software como WAF, DLP o CASB (no),
21. RS-SN-01 pruebas de penetración externas (parcial, solo internas),
22. RS-SN-02 ubicación UE de data centers (no, fuera de la UE),
23. RS-SN-03 identificación de hosting y geolocalización (sí, pero incompleta),
24. RS-SN-04 funciones de gestión de activos para cliente (no),
25. RS-IA-01 limitación de funcionalidades de IA (parcial),
26. RS-IA-02 monitorización de complementos IA (no),
27. RS-IA-03 detección de anomalías IA/DoS (sí, básica),
28. RS-IA-04 firma digital/verificación modelos IA (no),
29. RS-IA-05 aplicación de parches en IA (parcial, manual),
30. RS-IA-06 protección frente a filtración de datos confidenciales en IA (no),
31. RS-IA-07 filtrado y saneamiento de datos externos en IA (parcial),
32. RS-IA-08 evaluación de cumplimiento regulatorio en IA (no),
33. RS-IA-09 certificación ISO 42001 u otra relacionada con IA (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.