IS 2.d.02 (a) - Auditoría de Superficie de Exposición Post-Incidente (OSINT pasivo)

- Entidad objetivo: Clínica de San Rafael de Cádiz
- Equipo/Grupo: [Nombre del grupo]
- Integrantes: [Nombre Apellido (Iniciales)], [..]
- Fecha(s) de investigación: [YYYY-MM-DD a YYYY-MM-DD]
- Versión: 1.0
- Límite de entrega (a): máximo 6 folios (12 caras) en PDF (si aplica)

1. Resumen ejecutivo

Objetivo. Determinar qué información pública existía (antes del incidente supuesto) que podría haber facilitado la fase de reconocimiento de un atacante: identidades digitales, contactos, dominios/subdominios, huella documental (metadatos), menciones públicas y exposiciones derivadas.

Hallazgos clave (3-7 bullets). - [Hallazgo 1 + por qué importa] - [Hallazgo 2 + por qué importa] - [Hallazgo 3 + por qué importa]

Riesgo global (una frase). - [Bajo/Medio/Alto] por [motivo principal].

Recomendaciones prioritarias (3-5 bullets). - [Acción 1] - [Acción 2] - [Acción 3]

2. Alcance, supuestos y reglas de compromiso

Alcance. Solo OSINT pasivo sobre la entidad (y su huella pública asociada). No se incluye investigación individual (apartado b).

Fuentes permitidas (ejemplos). Motores de búsqueda, hemeroteca, registros públicos, perfiles públicos en RRSS, repositorios públicos, documentos públicos, Wayback/archivos, bases de datos de brechas (consulta pasiva).

Regla crítica. Prohibida cualquier acción activa: escaneos, enumeración directa de servicios, pruebas de login, interacción con formularios, generación de tráfico hacia los sistemas objetivo.

Minimización y privacidad. - Evitar incluir datos personales innecesarios. - Si aparecen datos personales de terceros (p. ej., correos de empleados), aplicar reducción: mostrar solo lo imprescindible o enmascarar parcialmente cuando no aporte valor al riesgo.

3. Metodología (ciclo OSINT)

Esta sección describe el proceso seguido según el ciclo OSINT: planificación, fuentes, adquisición, procesamiento, análisis y difusión.

3.1 Planificación y dirección

- Preguntas guía (ejemplos):
  - ¿Qué dominios y marcas usa la entidad?
  - ¿Existen patrones de email/usuarios visibles públicamente?
  - ¿Existen documentos públicos con metadatos reveladores?
  - ¿Hay menciones de tecnologías, proveedores, sedes, organigrama o personal?
  - ¿La entidad aparece asociada a brechas pasadas o leaks públicos?
- Criterios de priorización:
  - Impacto potencial en ingeniería social.
  - Reutilización de credenciales/patrones.
  - Exposición de infraestructura por huella documental/histórica.
- Ventana temporal:
  - Consulta realizada en: [YYYY-MM-DD]
  - Evidencias archivadas en: `evidencias/`, no obstante deben quedar enlazadas en el informe.

3.2 Identificación de fuentes

Tabla de fuentes (añadir/quitar según aplique):

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
Buscadores	Google / Bing / DuckDuckGo	menciones, PDFs, indexación	dorks sin acceder a paneles
Archivo web	Wayback Machine	versiones antiguas	solo lectura
Dominios	WHOIS/RDAP (consulta)	datos de registro	solo consulta pública
DNS pasivo	dnsdumpster, securitytrails, etc.	subdominios/histórico	sin enumeración activa
Brechas	HIBP / DeHashed (si se usa)	apariciones en brechas	no intentar logins
RRSS	LinkedIn/X/Facebook (público)	perfiles, roles, nicks	solo contenido público
Metadatos	exiftool/FOCA (sobre docs públicos)	autores, rutas, software	sobre ficheros públicos

3.3 Adquisición (recopilación)

- Consultas realizadas (resumen):
  - [Query/dork 1]
  - [Query/dork 2]
  - [Query/dork 3]
- Evidencias:
  - Guardar capturas o PDFs en `evidencias/` con nombres: `YYYY-MM-DD_fuente_tema.ext`
  - Registrar URL (más capturas) y fecha de acceso en cada hallazgo.
  - Toda evidencia mencionada en el informe debe estar enlazada (URL y/o ruta relativa a `evidencias/`).

3.4 Procesamiento y organización

- Normalización:
  - Deduplicación de correos/teléfonos/dominios.
  - Agrupación por categoría (contacto, identidad, infra, documentos).
- Criterios de calidad:
  - Fiabilidad de la fuente (primaria vs. terciaria).
  - Fecha y vigencia (actual vs. histórico).
  - Corroboración cruzada (>= 2 fuentes cuando sea posible).

3.5 Análisis e interpretación

- Correlaciones (ejemplos):
  - Patrones de email + nombres de empleados + roles (posible spear phishing).
  - Documentos públicos -> metadatos -> nombres de usuario/software.
  - Dominios/subdominios históricos -> superficies olvidadas.
- Valoración de riesgo: usar una escala simple.
  - Alto: facilita acceso/engaño de alta probabilidad o alto impacto.
  - Medio: aporta información útil, pero requiere pasos adicionales.
  - Bajo: información marginal o muy genérica.

3.6 Difusión

- Este informe resume hallazgos, evidencia y recomendaciones accionables.
- Presentación clara para audiencias técnicas y no técnicas.

4. Herramientas utilizadas

Herramienta	Tipo	Uso concreto	Salida/evidencia
[Herramienta]	[Buscador/DNS/Metadatos/etc.]	[Para que]	[archivo en evidencias/ o URL]

5. Resultados (hallazgos)

Formato recomendado por hallazgo:

Campo	Contenido
ID	A-01
Categoría	Contacto / Identidad / Dominio-DNS / Documentos-Metadatos / RRSS / Brechas
Descripción	[Qué se encontró, claro y verificable]
Evidencia	[URL] + `evidencias/...`
Fecha evidencia	[YYYY-MM-DD]
Impacto	[Qué permite a un atacante]
Riesgo	Alto / Medio / Bajo
Recomendación	[Mitigación concreta]

5.1 Identidades digitales (nicks, perfiles, cuentas)

- A-01
- A-02

5.2 Datos de contacto (emails, teléfonos, estructuras)

- A-03
- A-04

5.3 Dominios, subdominios y huella DNS (pasivo)

- A-05
- A-06

5.4 Huella documental y metadatos (documentos públicos)

- A-07
- A-08

5.5 Brechas y filtraciones (consulta pasiva)

- A-09

6. Resumen de riesgos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-01	[..]	Alto	P1	[..]
A-02	[..]	Medio	P2	[..]
A-03	[..]	Bajo	P3	[..]

7. Conclusiones

- [Conclusión 1: qué explica la exposición encontrada y por qué importa]
- [Conclusión 2]
- [Conclusión 3]

8. Recomendaciones

Quick wins (0-30 días) - [..] - [..]

Medio plazo (1-3 meses) - [..]

Mejora continua - [..]

9. Anexos

9.1 Registro de fuentes

Fuente	URL	Fecha acceso	Nota
[Fuente]	[..]	[YYYY-MM-DD]	[..]

9.2 Consultas (dorks) empleadas

(Registrar aquí las consultas utilizadas. Evitar incluir acciones activas o instrucciones de acceso.)

- `site:[dominio] filetype:pdf [palabra clave]`
- `site:[dominio] "@[dominio]"`
- `"Clínica San Rafael" "Cádiz" [palabra clave]`

9.3 Evidencias (índice)

- `evidencias/`:
  - `YYYY-MM-DD_fuente_tema.ext` - [descripción]