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

- **Entidad objetivo:** Clínica de San Rafael de Cádiz
- **Equipo/Grupo:** Grupo 3
- **Integrantes:** José María Escalón Prada, Abel García Domínguez, David Jiménez Ruiz
- **Fecha(s) de investigación:** 29/01/2026
- **Versión:** 1.0
- **Límite de entrega (a):** máximo 6 folios (12 caras) en PDF (si aplica)

1. Resumen ejecutivo

El presente informe detalla los resultados de una auditoría de inteligencia de fuentes OSINT pasiva realizada sobre la infraestructura digital y el footprinting del Hospital San Rafael de Cádiz.

El propósito de la investigación ha sido simular la fase de reconocimiento después de un ciberataque sufrido por la entidad, por lo que hemos identificado información pública que los atacantes puedan haber utilizado en su intrusión.

Objetivo. Determinar qué activos de información pública (identidades digitales, metadatos, infraestructura de red y datos organizativos) se encontraban expuestos antes del incidente supuesto, facilitando operaciones de ingeniería social o reconocimiento técnico por parte de un actor malintencionado.

Hallazgos clave.

- **Exposición de perfiles digitales (A-01, A-02):** Se han correlacionado perfiles profesionales con cuentas personales en redes sociales (Facebook, Instagram), revelando información familiar y privada utilizable para *pretexting*
- **Listado de personal (A-05):** La web corporativa publica un listado del personal, que ha podido permitir su raspado para hacer OSINT automatizado y campañas de phishing.
- **Transparencia de infraestructura física (A-09,A-10):** Wordpress y jquery son conocidos por tener brechas de seguridad muy graves.
- **Dominios, subdominios (A-06, A-07):** Información pública de DNS, whois que facilita conocer y entender la infraestructura a posibles agresores.

Riesgo global.

- **Alto**, debido principalmente a la exposición detallada de la estructura organizativa y datos personales del equipo médico, cosa que aumenta enormemente la superficie para ataques de ingeniería social dirigidos.

Recomendaciones prioritarias.

- **Minimización de datos del personal:** Retirar los listados completos de empleados del sitio web y establecer políticas de privacidad en redes sociales corporativas y personales.
- **Ofuscación de infraestructura:** Eliminar planos detallados y versiones de software (fingerprinting) de las cabeceras y metadatos públicos.
- **Higiene digital en documentos:** Implementar procesos de sanitización de metadatos (limpieza de usuarios y software) en todos los archivos PDF antes de su publicación.

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. Se han empleado motores de búsqueda generalistas, registros de dominio públicos (Whois), repositorios de DNS pasivo, redes sociales profesionales y personales, y análisis de metadatos en documentos indexados.

Regla crítica. Se ha prohibido cualquier acción activa, incluyendo escaneos de puertos, enumeración de servicios, intentos de autenticación, inyección de tráfico o interacción con formularios web que pudiera alertar a los sistemas objetivo o alterar su funcionamiento.

Minimización y privacidad.

- Se ha aplicado el principio de minimización de datos en la redacción del informe.
- Los datos personales de terceros (correos electrónicos, teléfonos personales) han sido ofuscados o reducidos parcialmente para demostrar el hallazgo sin incurrir en una exposición innecesaria, salvo cuando resultan indispensables para evidenciar el riesgo.

3. Metodología (ciclo OSINT)

Esta investigación se ha regido por las fases estándar del ciclo de inteligencia: planificación, identificación de fuentes, adquisición, procesamiento, análisis y difusión.

3.1 Planificación y dirección

- **Preguntas guía:**

    - ¿Qué nivel de detalle sobre la estructura organizativa es accesible desde la web corporativa?
    - ¿Es posible correlacionar identidades corporativas con perfiles privados en redes sociales?
    - ¿Existen metadatos en la documentación pública que revelen software interno o usuarios?
    - ¿Qué subdominios o servicios olvidados son visibles a través de registros DNS históricos?
- **Criterios de priorización:**
    - Impacto en la viabilidad de campañas de ingeniería social (*phishing*, *vishing*).
    - Exposición de versiones de software vulnerables.
    - Riesgo reputacional derivado de la exposición de datos personales.
- **Ventana temporal:**
    - Consulta realizada en: 01/02/2026
    - Evidencias archivadas en: evidencias/.

3.2 Identificación de fuentes

Tabla de fuentes empleadas durante la investigación:

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
Buscadores	Google	Archivos, listas, información de perfiles públicos de linkedin	Sin interacción directa con el hospital ni su personal
Web corporativa	https://www.hospitalespascual.com/	Archivos, listados de pacientes, números de teléfono	La web es pública y no requiere interacción más allá de observar el contenido existente
DNS	IntoDNS / DnsChecker	DNSs / dominios	Sin consultas directas al servidor DNS
Dominios	Whois	Datos de registro y propiedad	Contenido público
RRSS	LinkedIn, Facebook, Instagram	Perfiles, relaciones, actividad	Análisis de contenido público
Búsqueda de versiones pasadas	Wayback Machine	Versiones anteriores de la web, con credenciales o datos expuestos	Wayback machine no interactua con el objetivo de ninguna manera

3.3 Adquisición (recopilación)

- **Consultas realizadas (resumen):**
    - **Dorks Genéricos (Descubrimiento)**
        - site:linkedin.com/in/ "Hospital San Rafael" "Cádiz" (Administrativo OR Administración OR Gestión OR Director OR Gerente OR RRHH)
        - Buscar personal de "Hospitales Pascual" en Cádiz (Grupo matriz):
        - site:linkedin.com/in/ "Hospitales Pascual" "Cádiz" (Administración OR Director)
        - site:hospitalespascual.com filetype:pdf
        - site:hospitalespascual.com/hospital-san-rafael filetype:pdf
        - "Clínica San Rafael" "Cádiz" site:facebook.com
    - **Para Ignacio Ortiz Acero (Director Médico)**
        - site:linkedin.com/in/ "Ignacio Ortiz Acero"
        - site:linkedin.com "Ignacio Ortiz Acero" "Cádiz"
        - site:linkedin.com "Ignacio Ortiz Acero" "San Rafael"
    - **Para Irene Moya García (Directora de Administración)**
        - site:linkedin.com/in/ "Irene Moya García"
        - site:linkedin.com "Irene Moya García" "Administración"
        - site:linkedin.com "Irene Moya García" "Hospitales Pascual”
- **Evidencias:**
    - Cada hallazgo referenciado en este informe incluye su correspondiente enlace a la evidencia local o URL fuente.

3.4 Procesamiento y organización

- **Normalización:**
    - Se han descartado duplicados en los resultados de búsqueda.
    - La información se ha categorizado en: Identidad, Contacto, Infraestructura Técnica y Huella Documental.
- **Criterios de calidad:**
    - Se ha verificado la vigencia de la información (descartando datos obsoletos no relevantes).
    - Se ha buscado la corroboración cruzada (validar un dato en al menos dos fuentes independientes, ej. Web corporativa + LinkedIn).

3.5 Análisis e interpretación

- **Correlaciones identificadas:**
    - **Identidad + RRSS:** La obtención de nombres completos en la web oficial permitió localizar perfiles en Facebook e Instagram con configuración de privacidad abierta, exponiendo datos familiares útiles para la extorsión o el engaño.
    - **Documentos + Metadatos:** El análisis de PDFs corporativos reveló usuarios del sistema y versiones de software de generación de documentos.

    - **Infraestructura + Versiones:** La inspección pasiva de cabeceras HTTP y código fuente expuso el uso de CMS WordPress y librerías jQuery específicas.
- **Valoración de riesgo:**
    - **Alto:** Información que habilita ataques directos (ingeniería social creíble, acceso físico).
    - **Medio:** Información técnica que facilita la enumeración de vulnerabilidades.
    - **Bajo:** Datos genéricos o de bajo impacto operativo.

3.6 Difusión

- Este informe técnico presenta los hallazgos de forma estructurada para permitir a la dirección del Hospital San Rafael evaluar su postura de seguridad y aplicar las medidas correctoras propuestas.

4. Herramientas utilizadas

Herramienta	Tipo	Uso concreto	Salida/evidencia
Google	Buscador	Localización de empleados y documentos	Sin salida específica
IntoDNS / DnsChecker	DNS/Dominio	Enumeración pasiva de subdominios y Whois	evidencias/dominios-reportes/IntoDNS.png evidencias/dominios-reportes/dns.png
DevTools (Browser)	Análisis Web	Identificación de tecnologías (Wappalyzer pasivo)	evidencias/vulnerabilidades/Wordpress.png
Script de Python	Extracción de datos	Extracción de datos de la página de personal	hospital_personnel_hospital-san-rafael_past.json hospital_personnel_hospital-san-rafael_present.json scrape-personnel.py
WhoIS	Dominio/extracción de datos	Extracción de datos de la página principal del hospital	evidencias/dominios-reportes/whois.png

Wayback machine	Búsqueda de vulnerabilidades pasadas	Búsqueda de información relevante en versiones anteriores	https://web.archive.org/web/20231003001212/https://www.hospitalespascual.com/hospital-san-rafael/

5. Resultados (hallazgos)

A continuación, se detallan las exposiciones identificadas, clasificadas por categoría.

5.1 Identidades digitales (nicks, perfiles, cuentas)

- **A-01**

Campo	**Contenido**
ID	A-01
Categoría	Identidad digital
Descripción	Perfiles en redes sociales del director de la clínica Ignacio Ortiz Acero, incluyendo su clínica privada, perfil de colegiado y linkedin
Evidencia	clinica_ignacio_ortiz_acero.png, colegio_medicos_ignacio_ortiz_acero.png, linkedin_ignacio_ortiz_acero.png
Fecha evidencia	01/02/2026
Impacto	El perfil público del director de la clínica expone mucha información, incluso sin hacer análisis profundos ni cotejar con bases de fugas de datos.
Riesgo	**Alto**
Recomendación	Limitar la cantidad de información que se facilita del director de la clínica

- **A-02**

Campo	**Contenido**
ID	A-02
Categoría	Identidad digital

Descripción	OSINT sobre Irene Moya García, para buscar el contenido existente sobre ella en redes sociales.
Evidencia	Linkedin
Fecha evidencia	01/02/2026
Impacto	La agregación de fuentes permite la suplantación de identidad profesional y facilita ataques de *phishing* dirigidos basados en su actividad reciente.
Riesgo	**Medio**
Recomendación	Unificar y controlar la huella digital profesional; separar estrictamente los perfiles lúdicos de los profesionales.

5.2 Datos de contacto (emails, teléfonos, estructuras)

- **A-03**

Campo	**Contenido**
ID	A-03
Categoría	Contacto
Descripción	La "Guía de Usuario" alojada en la web contiene un directorio detallado de contactos internos, exponiendo canales directos de comunicación.
Evidencia	Guía PDF, Captura 1, Captura 2
Fecha evidencia	01/02/2026
Impacto	Facilita la recolección de correos y teléfonos para campañas de spam o phishing masivo.
Riesgo	**Medio**
Recomendación	Publicar solo contactos genéricos (tipo *info@*) y no listas detalladas de extensiones internas.

- **A-04**

Campo	**Contenido**

ID	A-04
Categoría	Contacto
Descripción	La página "Sobre nosotros" expone mucha información personal.
Evidencia	Guía Web + Captura
Fecha evidencia	01/02/2026
Impacto	Ampliación de la superficie de ataque para ingeniería social.
Riesgo	**Bajo**
Recomendación	Revisar la necesidad operativa de exponer esta información directamente en web pública.

- **A-05**

Campo	**Contenido**
ID	A-05
Categoría	Listado de personal
Descripción	Listado de personal completo tanto pasado como presente
Evidencia	personal pasado, personal presente
Fecha evidencia	01/02/2026
Impacto	Este listado creado en formato json contiene dos listados de personal. Un listado obtenido de la web antigua del hospital en
Riesgo	**Alto**
Recomendación	Limitar la cantidad de información que se facilita del personal. El personal de administración no tiene por qué estar en la lista de personal médico.

5.3 Dominios, subdominios y huella DNS (pasivo)

- **A-06**

Campo	**Contenido**
ID	A-06
Categoría	Dominio-DNS
Descripción	Información de registro Whois pública, revelando datos técnicos y administrativos del dominio.
Evidencia	Whois Report
Fecha evidencia	01/02/2026
Impacto	Facilita la identificación de proveedores de hosting y fechas de expiración para ataques de *domain hijacking*.
Riesgo	**Bajo**
Recomendación	Activar la protección de privacidad (Whois Privacy) en el registrador de dominios.

- **A-07**

Campo	**Contenido**
ID	A-07
Categoría	Dominio-DNS
Descripción	Mapeo de la huella DNS completa (registros MX, TXT, A) mediante consultas pasivas.
Evidencia	IntoDns
Fecha evidencia	01/02/2026
Impacto	Permite a un atacante comprender la arquitectura de red y los proveedores de correo y servicios externos.
Riesgo	**Alto**

Recomendación	Minimizar TXT/SPF innecesarios, implementar DMARC estricto (p=reject), rotar IPs/NS, ocultar SOA mínimo y monitorear con herramientas como dnsdumpster.

- **A-08**

Campo	**Contenido**
ID	A-08
Categoría	Dominio-DNS
Descripción	Mapeo de la huella DNS completa (registros MX, TXT, A) mediante consultas pasivas.
Evidencia	DnsChecker
Fecha evidencia	01/02/2026
Impacto	Permite a un atacante comprender la arquitectura de red y los proveedores de correo y servicios externos.
Riesgo	**Medio**
Recomendación	Minimizar la información en registros TXT y revisar configuraciones SPF/DMARC.

5.4 Vulnerabilidades (consulta pasiva)

- **A-09**

Campo	**Contenido**
ID	A-09
Categoría	Brechas Tecnológicas
Descripción	Análisis pasivo del código fuente y cabeceras que revela el uso de **WordPress**
Evidencia	WordPress
Fecha evidencia	01/02/2026
Impacto	Permite la búsqueda de vulnerabilidades conocidas (CVEs) asociadas a versiones específicas (*fingerprinting*).

Riesgo	**Medio**
Recomendación	Ocultar versiones en cabeceras HTTP y mantener el CMS actualizado.

- **A-10**

Campo	**Contenido**
ID	A-10
Categoría	Brechas Tecnológicas
Descripción	Análisis pasivo del código fuente y cabeceras que revela el uso de la librería **jQuery** con sus versiones específicas.
Evidencia	jQuery
Fecha evidencia	01/02/2026
Impacto	Permite la búsqueda de vulnerabilidades conocidas (CVEs) asociadas a versiones específicas (*fingerprinting*).
Riesgo	**Alto**
Recomendación	Ocultar versiones en cabeceras HTTP y mantener el CMS actualizado.

6. Resumen de riesgos

ID	**Hallazgo (resumen)**	**Riesgo**	**Prioridad**	**Acción recomendada**
A-01 / A-02	Exposición de perfiles personales (Facebook/Instagram) correlacionados con roles corporativos.	Alto	P1	Concienciación sobre privacidad en RRSS y separación estricta de perfiles personales/profesionales.
A-05	Publicación de listado completo del personal ("Equipo humano") facilitando *scraping* y *phishing*.	Alto	P1	Retirar listados nominativos públicos o restringir su acceso mediante autenticación.

A-09 / A-10	Identificación de versiones de software vulnerables (WordPress, jQuery) mediante *fingerprinting* pasivo.	Medio	P2	Ocultar versiones en cabeceras HTTP y mantener una política estricta de actualizaciones de seguridad.
A-06 / A-07	Información técnica de infraestructura (DNS, Whois) expuesta públicamente.	Medio	P2	Activar privacidad Whois y minimizar la información en registros DNS públicos.
A-03 / A-04	Documentos públicos con metadatos (usuarios, software) o información interna sensible.	Bajo	P3	Implementar procesos de sanitización de metadatos en documentos PDF antes de su publicación.
A-08	Directorio físico y planos de la instalación accesibles en la web.	Bajo	P3	Evaluar la necesidad de publicar planos detallados que faciliten el reconocimiento físico.

7. Conclusiones

- **Perfiles e identidades públicos y desprotegidos:** La información disponible sobre los trabajadores, ya sean personal sanitario o no, es enorme, facilitando el raspado masivo de datos de personal, suficiente para hacer procesos de OSINT sobre potenciales objetivos, con el fin de plantear campañas de phishing, spear phishing o whaling.
- **Infraestructura y organización descubierta:** La división en departamentos, así como teléfonos, correos y nombres y estructura física del edificio es pública y detallada, facilitando la comprensión de la organización
- **Información técnica disponible con fuentes abiertas**: versiones, tecnologías, servidores, etc

8. Recomendaciones

Basándonos en los hallazgos y el nivel de riesgo identificado, se proponen las siguientes medidas:

Quick wins (0-30 días)

Medidas de implementación inmediata y bajo coste para cerrar las brechas más críticas.

- Eliminación de listados nominativos (A-05): Recortar la sección pública "Equipo humano" de la web corporativa para retirar a personal administrativo o de menor relevancia pública.
- Ofuscación de versiones de software (A-09, A-10): Configurar el servidor web y el CMS (WordPress) para eliminar las cabeceras HTTP y meta-etiquetas que revelan versiones específicas de software y plugins (jQuery, etc.), dificultando el fingerprinting.
- Limpieza de metadatos (A-03, A-04): Ejecutar un proceso de sanitización (scrubbing) sobre todos los documentos PDF actualmente alojados en la web para eliminar información innecesaria, además de autores, rutas de red y software de creación.
- Simplificación del directorio físico (A-08): Modificar la información del directorio web para mostrar sólo ubicaciones genéricas de atención al paciente, eliminando detalles estructurales internos (ubicación de servidores, despachos específicos o controles de enfermería).

Medio plazo (1-3 meses)

Cambios estructurales, normativos y de concienciación.

- Campaña de "Higiene Digital" para empleados (A-01, A-02): Impartir formación específica al personal sanitario y administrativo sobre los riesgos de la exposición en redes sociales (Facebook, Instagram, Linkedin). El objetivo es concienciar sobre cómo la información puede ser usada para atacar a la entidad.
- Protocolo de publicación segura: Establecer un procedimiento obligatorio que incluya la revisión y eliminación de metadatos y datos personales antes de subir cualquier nuevo documento o noticia a la web corporativa.

Mejora continua

Mantenimiento de la postura de seguridad a largo plazo.

- Monitorización de huella digital: Implementar alertas automáticas (Google Alerts o herramientas de Threat Intelligence) para detectar nuevas menciones de directivos o fugas de documentos corporativos en repositorios públicos.
- Auditorías OSINT recurrentes: Realizar este mismo ejercicio de auditoría pasiva de forma trimestral para comprobar que las medidas aplicadas se mantienen y que no han surgido nuevas superficies de exposición con los cambios en la web.

9. Anexos

9.1 Registro de fuentes

Fuente	URL	Fecha acceso	Nota
Web Corporativa	https://www.hospitalespascual.com/	01/02/2026	Fuente primaria: listados, PDF y teléfonos.
Google	https://www.google.com	01/02/2026	Búsqueda de archivos indexados y perfiles públicos.
IntoDNS	https://intodns.com/	01/02/2026	Análisis pasivo de configuración DNS (A-07).
DNSChecker	https://dnschecker.org/	01/02/2026	Verificación de propagación y registros DNS (A-08).
Whois	https://who.is/	01/02/2026	Datos de registro de dominio y propiedad.
Wayback Machine	https://web.archive.org/	01/02/2026	Búsqueda de versiones históricas y fugas pasadas.
LinkedIn	https://www.linkedin.com/	01/02/2026	Identificación de perfiles profesionales (A-01, A-02).

Facebook	https://www.facebook.com/	01/02/2026	Análisis de perfiles personales abiertos (A-01).
Doctoralia	https://www.doctoralia.es/	01/02/2026	Datos de consultorios privados cruzados.

9.2 Consultas (dorks) empleadas

- **Dorks Genéricos**
  - site:linkedin.com/in/ "Hospital San Rafael" "Cádiz" (Administrativo OR Administración OR Gestión OR Director OR Gerente OR RRHH)
  - Buscar personal de "Hospitales Pascual" en Cádiz (Grupo matriz):
  - site:linkedin.com/in/ "Hospitales Pascual" "Cádiz" (Administración OR Director)
  - site:hospitalespascual.com filetype:pdf
  - site:hospitalespascual.com/hospital-san-rafael filetype:pdf
  - "Clínica San Rafael" "Cádiz" site:facebook.com
- **Para Ignacio Ortiz Acero (Director Médico)**
  - site:linkedin.com/in/ "Ignacio Ortiz Acero"
  - site:linkedin.com "Ignacio Ortiz Acero" "Cádiz"
  - site:linkedin.com "Ignacio Ortiz Acero" "San Rafael"
- **Para Eva Reyes Pérez (Directora de Enfermería)**
  - site:linkedin.com/in/ "Eva Reyes Pérez"
  - site:linkedin.com "Eva Reyes Pérez" "Enfermería" "Cádiz"
  - site:linkedin.com "Eva Reyes Pérez" "San Rafael"
- **Para Irene Moya García (Directora de Administración)**
  - site:linkedin.com/in/ "Irene Moya García"
  - site:linkedin.com "Irene Moya García" "Administración"
  - site:linkedin.com "Irene Moya García" "Hospitales Pascual"

9.3 Evidencias (índice)

- evidencias/:
  - personal/
    - hospital_personnel_hospital-san-rafael_past.json
    - hospital_personnel_hospital-san-rafael_present.json
    - scrape-personnel.py
    - clinica_ignacio_ortiz_acero.png
    - colegio_medicos_ignacio_ortiz_acero.png

        - linkedin_ignacio_ortiz_acero.png
        - linkedin_irene_moya_garcia.png
    - vulnerabilidades/
        - Wordpress.png
        - Jquery.png
    - contacto/
        - contacto1.png
        - contacto2.png
        - equipo humano.png
    - dominios-reportes/
        - WHOis.png
        - dns.png
        - ev1.png
        - DatosHospital.png
        - IntoDNS.png