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 5
- ***Integrantes:*** Sergio González Noria (SGN), Iván Paúl Alba (IPA), Manuel Pérez Romero (MPR), Javier Calvillo Acebedo (JCA).
- ***Fecha(s) de investigación:*** 2026-01-28 a 2026-02-01
- ***Versión:*** 1.0
- ***Límite de entrega (a):*** máximo 6 folios (12 caras) en PDF (si aplica)

1. Resumen ejecutivo

Objetivo. En este trabajo hemos investigado qué información del Hospital San Rafael de Cádiz está disponible públicamente en Internet y que un posible atacante podría usar para preparar un ataque: datos de empleados, correos, teléfonos, páginas web, documentos públicos, etc.

Principales hallazgos: - Encontramos información personal de 10 empleados en Internet: teléfonos, correos y apodos en redes sociales. Esta información podría permitir a alguien hacerse pasar por ellos o engañar a otros empleados. - Descubrimos que el hospital utiliza 4 servidores para gestionar sus dominios (dns1, dns2, dns3 y dns4.sered.net), todos gestionados por la misma empresa externa. - Hay varias páginas web relacionadas con el hospital: mail.hospitalespascual.com y correo.hospitalespascual.com para el correo, y además una página de pruebas (www.test.hospitalespascual.com) que no debería estar visible públicamente. - El hospital publica en su web detalles de los equipos médicos que utilizan (escáneres, resonancias, etc.), lo que podría ayudar a alguien a conocer la tecnología disponible. - También encontramos datos personales como dónde estudiaron algunos empleados, direcciones de sus consultas privadas y números de colegiado.

Nivel de riesgo:
- Consideramos que el riesgo es **ALTO**, porque hay mucha información personal de los empleados accesible, se puede ver toda la infraestructura digital del hospital y además hay una página de pruebas pública que cualquiera puede encontrar.

Recomendaciones principales: - Quitar o ocultar la información personal de los empleados en Internet (teléfonos, correos personales, direcciones).
- Cerrar o proteger la página de pruebas (test.hospitalespascual.com) que no debería ser pública.
- Dar formación sobre ciberseguridad a los empleados con información más expuesta.
- Evitar publicar tantos detalles técnicos sobre los equipos médicos en la web pública.
- Crear unas normas internas sobre qué información se puede publicar y cuál no.

2. Alcance, supuestos y reglas de compromiso

Alcance

Se ha realizado únicamente OSINT pasivo sobre la Clínica San Rafael de Cádiz y su huella pública asociada, es decir, toda la información accesible en Internet relacionada con la entidad: dominios y subdominios, registros DNS históricos, certificados, datos de contacto, perfiles públicos de empleados y menciones en la web.

No se incluye investigación individual (apartado b) ni se ha interactuado con los sistemas de la clínica en ningún momento.

Fuentes utilizadas

- Google Search (búsquedas generales y Google Dorks)
- crt.sh (certificados públicos)
- dnsdumpster.com (DNS pasivo e histórico)
- Have I Been Pwned (consulta de correos y dominio en brechas)
- Sherlock (búsqueda de nicks en redes sociales)
- TinEye (búsqueda inversa de imágenes)
- Epieos (consultas pasivas de correos y perfiles)

- PimEyes (búsqueda facial sobre imágenes públicas)

Todas estas herramientas se consultaron de forma pasiva, utilizando únicamente información ya disponible públicamente y sin generar tráfico hacia los sistemas de la clínica.

Regla crítica

No se realizaron acciones activas: no se hicieron escaneos de puertos, pruebas de login, enumeración directa de servicios ni interacción con formularios o sistemas de la entidad.

En aquellas herramientas que pueden tener funciones activas, solo se usaron los resultados pasivos que la propia plataforma ofrecía (por ejemplo, dnsdumpster o crt.sh).

Minimización y privacidad

- Evitar incluir datos personales innecesarios en el informe.
- Si aparecen datos de terceros (por ejemplo, correos de empleados), aplicar reducción: mostrar solo lo imprescindible o enmascararlos cuando no aporten valor al análisis.

3. Metodología (cómo hicimos la investigación)

En esta sección explicamos los pasos que seguimos para llevar a cabo nuestra investigación de manera ordenada y documentada.

3.1 Planificación

- Preguntas que nos hicimos al empezar:
  - ¿Qué páginas web usa el hospital?
  - ¿Podemos encontrar correos electrónicos o patrones de cómo crean los usuarios?
  - ¿Hay documentos públicos que puedan revelar información interna?
  - ¿Se menciona qué tecnologías usan, con qué empresas trabajan o quiénes son los empleados?
  - ¿Ha habido alguna filtración de datos del hospital en el pasado?
- Cómo decidimos qué era importante:
  - Información que podría usarse para engañar a alguien del hospital.
  - Patrones que se repiten (por ejemplo, cómo crean los usuarios o contraseñas).
  - Detalles de la infraestructura tecnológica que podrían ser útiles para un atacante.
- Cuándo hicimos la investigación:
  - Las búsquedas se realizaron entre el 15 de enero y el 1 de febrero de 2026.
  - Todas las capturas de pantalla, CSV y evidencias se guardaron en la carpeta `evidencias/` con la fecha y descripción del hallazgo.

3.2 Fuentes que consultamos

Estas son las herramientas que usamos y cómo las empleamos de forma pasiva:

Tipo de fuente	Herramienta utilizada	Para qué la usamos	Cómo la usamos (sin interactuar con sistemas)
Buscadores	Google / Bing / DuckDuckGo	Buscar documentos y menciones del hospital	Búsquedas normales, sin intentar acceder a paneles privados
Páginas antiguas	Wayback Machine	Ver cómo era la web anteriormente	Solo lectura de archivos históricos
Dominios	WHOIS (consulta pública)	Ver quién registró el dominio	Solo consulta pública, no intentamos modificar nada
DNS	dnsdumpster, crt.sh	Identificar subdominios y servidores	Consultas pasivas a bases de datos públicas
Filtraciones	Have I Been Pwned	Revisar si hubo filtraciones de datos	Solo consulta pasiva, no intentamos usar credenciales
Redes sociales	LinkedIn / Facebook (público)	Buscar perfiles de empleados	Solo lo que es público

Documentos	Análisis de PDFs públicos	Ver autores, software y metadatos	Solo documentos ya publicados

3.3 Búsquedas que hicimos

- Ejemplos de búsquedas en Google y otros buscadores:
  - PDFs del hospital.
  - Correos que terminan en `@hospitalespascual.com`.
  - Nombres de empleados mencionados públicamente.
- Cómo registramos las pruebas:
  - Capturas de pantalla con fecha y descripción.
  - Archivos CSV exportados de herramientas como SpiderFoot.
  - Todo guardado en la carpeta `evidencias/` para poder contrastar cada hallazgo.

3.4 Organización de la información

- Cómo ordenamos los datos:
  - Eliminamos duplicados (por ejemplo, un mismo teléfono encontrado en varias fuentes).
  - Agrupamos la información por categorías: datos de contacto, identidades, páginas web, documentos, etc.
- Cómo verificamos que la información era fiable:
  - Comprobamos que la fuente fuera de confianza.
  - Revisamos si la información estaba actualizada o era antigua.
  - Siempre que fue posible, contrastamos con al menos otra fuente para asegurarnos.

3.5 Análisis de lo que encontramos

- Conexiones importantes detectadas:
  - Correos + nombres + puestos de trabajo = alguien podría hacerse pasar por un jefe o compañero para engañar a empleados.
  - Documentos públicos revelan nombres de usuarios y programas internos.
  - Páginas web antiguas o de prueba accesibles públicamente podrían tener vulnerabilidades.
- Cómo decidimos el nivel de riesgo:
  - **Alto:** La información facilita mucho un ataque o engaño directo.
  - **Medio:** La información es útil para un atacante, pero requeriría pasos adicionales.
  - **Bajo:** Información general que aporta poco valor para un atacante.

3.6 Este informe

- Presentamos lo que encontramos, con pruebas y recomendaciones prácticas.
- Intentamos explicarlo de forma clara para que lo entienda cualquier persona, tenga conocimientos técnicos o no.
- Resume nuestro aprendizaje como estudiantes de ciberseguridad sobre cómo realizar un análisis OSINT pasivo.

4. Herramientas utilizadas

En esta sección listamos las herramientas que realmente usamos durante nuestra investigación, indicando para qué las usamos y qué evidencia guardamos de cada una.

Herramienta	Tipo	Uso concreto	Salida / evidencia
Google Search	Buscador	Búsqueda de dominios, subdominios, PDFs y menciones	-
crt.sh	Certificados SSL	Comprobación de certificados asociados a dominios	`evidencias/crtsh_hospitalespascual.png`
dnsdumpster.com	DNS pasivo	Identificación de subdominios y registros históricos	`evidencias/dnsdumpster_hospitalespascual.`

Herramienta	Tipo	Uso concreto	Salida / evidencia
Have I Been Pwned	Brechas de datos	Verificación de emails y dominios en filtraciones	-
Sherlock	Redes sociales / Identidad	Búsqueda de nicks y alias de empleados	-
TinEye	Búsqueda inversa de imágenes	Verificación de fotos públicas de empleados	`evidencias/2026-02-01_ExifTool1.png`
Epieos	Correo / perfiles	Consulta pasiva de correos y perfiles vinculados	`evidencias/2026-02-01_ExifTool2.png`
PimEyes	Reconocimiento facial	Verificación de imágenes públicas de empleados	`evidencias/2026-02-01_ExifTool3.png`
SpiderFoot	OSINT automatizado	Análisis de superficie digital, dominios, subdominios, certificados y hosting	`evidencias/SpiderFoot_HospitalSanRafael.`

5. Resultados (lo que encontramos)

A continuación detallamos cada descubrimiento importante que hicimos, con pruebas de dónde lo vimos y por qué creemos que es peligroso.

5.1 Identidades de empleados (apodos, perfiles, cuentas)

A-01: Dra. Ana De Lacour Juliá - **Categoría:** Identidad - **Qué encontramos:** Apodo en redes "anuskalaq", trabaja en Neurología, número de colegiado: 111107282 - **Dónde lo vimos:** Perfiles públicos profesionales - **Cuándo:** 20 de enero de 2026 - **Por qué es peligroso:** Alguien podría hacerse pasar por ella usando esta información para engañar a otros empleados - **Nivel de riesgo:** Alto - **Qué recomendamos:** Darle formación sobre cómo detectar intentos de engaño y activar la verificación en dos pasos en sus cuentas

A-02: Ignacio Ortiz Acero - **Categoría:** Identidad - **Qué encontramos:** Director Médico, apodo "sinueioa", número de colegiado: 111105853. Le gustan la Semana Santa, estudió en la Universidad de Cádiz y en Salesianos. Tiene un premio de una hermandad - **Dónde lo vimos:** Redes sociales y noticias locales - **Cuándo:** 20 de enero de 2026 - **Por qué es peligroso:** Es un cargo importante y hay mucha información personal. Alguien podría usar sus aficiones para ganarse su confianza y engañarle - **Nivel de riesgo:** Alto - **Qué recomendamos:** Avisarle de posibles intentos de manipulación basados en sus aficiones personales

A-03: Sandra Brenes Reyes - **Categoría:** Identidad - **Qué encontramos:** Psicóloga, número de colegiado AN08392. Tiene un Gmail personal (psicologasandrabrenes@gmail.com), teléfono móvil (693406050), dirección de su consulta (Avenida Buenavista 29, Vejer de la Frontera) y web personal - **Dónde lo vimos:** Página web personal y directorios de psicólogos - **Cuándo:** 22 de enero de 2026 - **Por qué es peligroso:** Su correo personal y teléfono están expuestos. Alguien podría contactarla haciéndose pasar por un paciente o colega - **Nivel de riesgo:** Alto - **Qué recomendamos:** Usar solo correo y teléfono del hospital para temas de trabajo y proteger mejor sus datos personales

A-04: Antonio Linares Moreno - **Categoría:** Identidad - **Qué encontramos:** Oncología Radioterápica, Nick "Tony Sugar" en luchawike.org, Núm. Colegiado: 111807100 - **Dónde lo vimos:** Foros temáticos - **Cuándo:** 25 de enero de 2026 - **Por qué es peligroso:** El nick permite rastrear actividad online y construir perfil personal - **Nivel de riesgo:** Medio - **Qué recomendamos:** Concienciación sobre separar identidad personal/profesional

A-05: Guido Weisman - **Categoría:** Identidad - **Qué encontramos:** Medicina Interna, Nicks "batataweis" y "gugaweis", Fellowship - **Dónde lo vimos:** Perfiles públicos en redes sociales - **Cuándo:** 25 de enero de 2026 - **Por qué es peligroso:** Múltiples nicks facilitan rastreo de actividad en distintas plataformas - **Nivel de riesgo:** Medio - **Qué recomendamos:** Revisar la información publicada y auditar presencia online

A-06: Otros empleados detectados - Camila Raduan Tozzini (Ginecología, Núm. Colegiado: 080865499) - Zulika Riveros (Podología, Tel: 956252624, Dirección: Avenida Padre de las Casas nº

4, Local 14, Cádiz) - Juan Manuel Fariñas Varo (Urología, varias direcciones de consultorios) - María Súnico Rodríguez (Psicología, Núm. Colegiado: AN06945, correo de la universidad: maria.sunico@uca.es) - Jorge Ortega García (Medicina Interna) - Manuel Casanova Ramón (Medicina Interna)

5.2 Datos de contacto (correos y teléfonos)

A-07: Teléfonos de empleados publicados - **Categoría:** Contacto - **Qué encontramos:** - 956017270 y 956048000 (Dra. Ana De Lacour Juliá) - 693406050 (Sandra Brenes Reyes - móvil personal) - 956252624 (Zulika Riveros) - **Dónde lo vimos:** Directorios médicos y páginas web públicas - **Cuándo:** 20 de enero de 2026 - **Por qué es peligroso:** Alguien podría llamar a los empleados haciéndose pasar por pacientes o colegas - **Nivel de riesgo:** Alto - **Qué recomendamos:** Que todas las llamadas pasen por la centralita del hospital

A-08: Correos electrónicos - **Categoría:** Contacto - **Qué encontramos:** - psicologasandrabrenes@gmail.com (Sandra Brenes - personal) - maria.sunico@uca.es (María Súnico - universidad) - **Dónde lo vimos:** Páginas web personales y directorios de universidades - **Cuándo:** 22 de enero de 2026 - **Por qué es peligroso:** Uso de cuentas externas, más fáciles de engañar - **Nivel de riesgo:** Alto - **Qué recomendamos:** Norma para usar solo correos del hospital (@hospitalespascual.com) para trabajo

5.3 Páginas web y servidores del hospital

A-09: Página web principal - **Categoría:** Páginas web - **Qué encontramos:** hospitalespascual.com (también hospital-san-rafael) - **Dónde lo vimos:** WHOIS y búsquedas en Google - **Cuándo:** 18 de enero de 2026 - **Por qué es peligroso:** No han registrado dominios parecidos, riesgo de typosquatting - **Nivel de riesgo:** Medio - **Qué recomendamos:** Registrar variantes comunes del dominio

A-10: Páginas adicionales - **Categoría:** Páginas web - **Qué encontramos:** - mail.hospitalespascual.com - correo.hospitalespascual.com - www.test.hospitalespascual.com (página de pruebas) - hospitalespascual.com.josemanuelpascualpascual.es (dominio ajeno) - **Dónde lo vimos:** crt.sh y dnsdumpster.com - **Cuándo:** 18 de enero de 2026 - **Por qué es peligroso:** La página de pruebas puede tener vulnerabilidades y el dominio ajeno puede confundir a usuarios - **Nivel de riesgo:** Alto - **Qué recomendamos:** Cerrar/proteger subdominio de pruebas y revisar el dominio ajeno

A-11: Servidores que gestionan la web - **Categoría:** Páginas web - **Qué encontramos:** 4 servidores de Sered en España - dns1.sered.net (185.37.231.10) - dns2.sered.net (46.175.128.146) - dns3.sered.net (193.84.177.223) - dns4.sered.net (193.84.177.125) - **Dónde lo vimos:** Consultas DNS públicas - **Cuándo:** 18 de enero de 2026 - **Por qué es peligroso:** Se conoce el proveedor y las IP, normal pero revisar configuración - **Nivel de riesgo:** Medio - **Qué recomendamos:** Mejorar seguridad (DNSSEC, limitar consultas)

5.4 Documentos e información publicada

A-12: Equipos médicos - **Categoría:** Información pública - **Qué encontramos:** Detalles de TAC, resonancias, endoscopias, ecógrafos, rayos X, laboratorios - **Dónde lo vimos:** Web oficial - **Cuándo:** 28 de enero de 2026 - **Por qué es peligroso:** Saber modelos exactos permite buscar vulnerabilidades conocidas - **Nivel de riesgo:** Medio - **Qué recomendamos:** Publicar información general sin detalles técnicos

A-13: Direcciones de consultorios - **Categoría:** Información pública - **Qué encontramos:** Direcciones privadas de algunos empleados - **Dónde lo vimos:** Directorios médicos y webs personales - **Cuándo:** 25 de enero de 2026 - **Por qué es peligroso:** Posible suplantación en persona - **Nivel de riesgo:** Medio - **Qué recomendamos:** Evaluar necesidad de publicar direcciones exactas

5.5 Filtraciones de datos (brechas de seguridad)

A-14: Consulta de filtraciones - **Categoría:** Filtraciones - **Qué encontramos:** - No se detectaron contraseñas filtradas de correos del hospital - Algunos correos personales (Sandra Brenes, María Súnico) no pudieron verificarse - **Dónde lo vimos:** Have I Been Pwned - **Cuándo:** 30 de enero de 2026 - **Por qué es buena noticia:** No hay contraseñas del hospital expuestas públicamente - **Nivel de riesgo:** Bajo - **Qué recomendamos:** Activar alertas de futuras filtraciones y verificación en dos pasos obligatoria para todos

6. Resumen de riesgos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-01	Subdominios sensibles y entornos de prueba accesibles públicamente (`test.hospitalespascual.com`, `www.test.hospitalespascual.com`)	Alto	P1	Restringir acceso a subdominios de test, aplicar autenticación o firewall, monitorizar tráfico externo y cerrar páginas innecesarias.
A-02	Información personal de empleados expuesta (nombres, apodos, correos, teléfonos, direcciones)	Alto	P1	Quitar o enmascarar información personal de empleados, formación sobre ciberseguridad, usar solo correos oficiales del hospital.
A-03	Páginas web y dominios no registrados o variantes del dominio principal disponibles	Medio	P2	Registrar variantes de dominio para prevenir typosquatting y confusión de usuarios.
A-04	Servidores visibles públicamente y certificados SSL expuestos	Medio	P2	Revisar configuración de servidores y certificados, limitar exposición de endpoints innecesarios, auditar servicios HTTPS, activar DNSSEC.
A-05	Detalles de equipos médicos publicados en web (modelos, especificaciones)	Medio	P2	Publicar información general sobre equipos sin dar detalles técnicos específicos que puedan aprovechar atacantes.
A-06	Direcciones de consultorios privados accesibles públicamente	Medio	P2	Evaluar la necesidad de publicar direcciones exactas, proteger información sensible de empleados.
A-07	Metadatos en documentos públicos (autores, rutas de software)	Bajo	P3	Sanear metadatos antes de publicar documentos, aplicar políticas internas de revisión de archivos.
A-08	Filtraciones pasadas de datos (de momento ninguna encontrada)	Bajo	P3	Activar alertas automáticas de futuras filtraciones y verificar cuentas con doble factor de autenticación.

7. Conclusiones

- La clínica tenía bastante **información personal de empleados accesible públicamente**: correos, teléfonos y direcciones de consultas, algo que hace más fácil que alguien intente engañarles mediante ingeniería social.
- Encontramos **subdominios de prueba y páginas extra** que están visibles en Internet, lo que podría dar pistas a un atacante sobre entornos de desarrollo o pruebas.
- La **infraestructura de correo y dominios** está completamente a la vista, con servidores y certificados SSL visibles, lo que facilita mapear cómo funciona todo el sistema de la clínica.

- Publicar **detalles técnicos de los equipos médicos y documentos con metadatos** también aumenta el riesgo, porque un atacante podría usar esa información para buscar vulnerabilidades conocidas o aprender cómo trabaja la clínica.

- En resumen, la **mezcla de datos de empleados, infraestructura visible y páginas de prueba** deja claros vectores que alguien podría usar para suplantación de identidad, phishing o intentar acceder a información sensible.

8. Recomendaciones

A continuación se presentan las recomendaciones organizadas por prioridad, alineadas con los hallazgos del apartado 6. Las acciones se clasifican en tres niveles temporales según su urgencia y el riesgo asociado.

8.1 Prioridad 1 (Urgente - 0 a 30 días)

Relacionado con A-01: Subdominios de prueba expuestos - [**IT/Seguridad**] Cerrar el acceso público a subdominios de prueba (`test.hospitalespascual.com`, `www.test.hospitalespascual.com`). Implementar autenticación mediante VPN o firewall que restrinja el acceso únicamente a IPs internas. - [**IT**] Auditar y documentar todos los subdominios activos del hospital. Eliminar los que no sean necesarios y proteger aquellos que deban mantenerse operativos. - [**IT**] Revisar el subdominio `hospitalespascual.com.josemanuelpascualpascual.es` para determinar su finalidad. Si no es legítimo, solicitar su eliminación o documentar su relación con la entidad.

Relacionado con A-02: Información personal de empleados expuesta - [**Comunicación/Web**] Retirar teléfonos directos, correos personales y direcciones físicas de empleados de todas las webs públicas. Publicar únicamente datos de contacto generales de la clínica (centralita, correo corporativo genérico). - [**RRHH**] Solicitar a los empleados identificados que migren todas las comunicaciones profesionales a correos corporativos (@hospitalespascual.com) y que eviten usar cuentas personales (Gmail, cuentas universitarias) para asuntos laborales. - [**RRHH/Seguridad**] Realizar una sesión de concienciación urgente para los 10 empleados identificados, explicando los riesgos de ingeniería social, suplantación de identidad y phishing dirigido. Incluir casos prácticos y señales de alerta. - [**RRHH**] Recomendar a empleados en puestos clave (especialmente Director Médico y personal con alta exposición) que limiten la información personal compartida públicamente en redes sociales y perfiles profesionales.

8.2 Prioridad 2 (Medio plazo - 1 a 3 meses)

Relacionado con A-03: Variantes de dominio no registradas - [**IT/Dirección**] Registrar variantes del dominio principal para prevenir ataques de typosquatting: `hospitalpascual.com`, `hospitalespascual.es`, `hospital-san-rafael.com`, entre otras similares. Configurar redirecciones al dominio oficial.

Relacionado con A-04: Infraestructura visible y certificados SSL - [**IT**] Revisar la configuración de los servidores DNS (dns1-4.sered.net) y activar DNSSEC para proteger contra ataques de envenenamiento de caché DNS. - [**IT**] Auditar los certificados SSL de todos los dominios y subdominios. Verificar fechas de caducidad y configurar alertas automáticas de renovación. - [**IT**] Limitar la exposición pública de endpoints innecesarios. Revisar qué servicios HTTPS están accesibles desde Internet y proteger aquellos que no deban ser públicos.

Relacionado con A-05: Detalles técnicos de equipos médicos - [**Comunicación/Web**] Revisar el contenido publicado sobre equipamiento médico en la web. Sustituir información técnica específica (modelos, especificaciones exactas) por descripciones genéricas de capacidades y servicios. - [**Dirección**] Establecer una política de publicación de información corporativa que incluya revisión de seguridad obligatoria antes de publicar contenidos sensibles.

Relacionado con A-06: Direcciones de consultorios privados - [**Comunicación**] Evaluar la necesidad de publicar direcciones exactas de consultorios privados asociados al hospital. Considerar la opción de publicar solo información de contacto general o zonas aproximadas. - [**Comunicación**] Crear un directorio de contacto controlado que evite exponer datos personales directos de empleados (teléfonos móviles, correos personales).

Medidas organizativas generales - [**RRHH**] Organizar un programa de formación en ciberseguridad para todo el personal, con especial énfasis en gestión de identidad digital, uso seguro de redes sociales

profesionales y detección de intentos de phishing. - [**IT**] Implementar autenticación multifactor (MFA/2FA) obligatoria para todos los empleados que accedan a sistemas corporativos, especialmente correo electrónico y sistemas internos. - [**Dirección**] Desarrollar una política formal de separación entre identidades personales y profesionales en redes sociales, con recomendaciones claras para empleados.

8.3 Prioridad 3 (Largo plazo - Mejora continua)

Relacionado con A-07: Metadatos en documentos públicos - [**IT/Comunicación**] Implementar un proceso de saneamiento de metadatos antes de publicar cualquier documento en la web (PDFs, imágenes, hojas de cálculo). Usar herramientas automatizadas para eliminar información de autores, rutas de archivos y software utilizado. - [**Dirección**] Establecer políticas internas de revisión de archivos antes de su publicación externa, incluyendo verificación de metadatos.

Relacionado con A-08: Monitorización de filtraciones - [**Seguridad/IT**] Suscribirse a servicios de monitorización de brechas de datos (ej. Have I Been Pwned Enterprise, servicios comerciales) que alerten automáticamente si el dominio @hospitalespascual.com o correos de empleados aparecen en filtraciones públicas. - [**Seguridad/IT**] Establecer un protocolo de respuesta ante detección de credenciales filtradas: cambio inmediato de contraseñas, revisión de accesos y auditoría de logs.

Medidas de monitorización y auditoría continua - [**Seguridad**] Realizar auditorías OSINT trimestrales (cada 3 meses) para identificar nueva información pública expuesta sobre la clínica, empleados o infraestructura. - [**RRHH/Seguridad**] Auditoría semestral (cada 6 meses) de la presencia digital de empleados en puestos críticos (dirección, acceso a datos sensibles, representantes públicos). - [**Seguridad**] Desarrollar un playbook de respuesta ante exposición de información sensible, incluyendo pasos de contención, notificación y mitigación. - [**IT**] Revisión anual de subdominios activos y servicios públicos, eliminando aquellos que no sean necesarios y documentando adecuadamente los que deban mantenerse.

9. Anexos

9.1 Registro de fuentes

Fuente	URL	Fecha acceso	Nota
Google Search	https://www.google.com	2026-01-28 a 2026-02-01	Búsquedas generales y Google Dorks sobre el hospital
crt.sh	https://crt.sh	2026-01-28 a 2026-02-01	Certificados SSL de dominios y subdominios
dnsdumpster.com	https://dnsdumpster.com	2026-01-28 a 2026-02-01	Información pasiva de subdominios y registros DNS
Have I Been Pwned	https://haveibeenpwned.com	2026-01-28 a 2026-02-01	Verificación de correos del hospital en filtraciones
Sherlock	https://github.com/sherlock-project/sherlock	2026-01-28 a 2026-02-01	Búsqueda de nicks y alias de empleados en redes sociales
TinEye	https://tineye.com	2026-01-28 a 2026-02-01	Búsqueda inversa de imágenes públicas de empleados

Fuente	URL	Fecha acceso	Nota
Epieos	https://epieos.com	2026-01-28 a 2026-02-01	Consulta pasiva de correos y perfiles
PimEyes	https://pimeyes.com/	2026-01-28 a 2026-02-01	Reconocimiento facial sobre imágenes públicas de empleados
Wayback Machine	https://archive.org/web/	2026-01-28 a 2026-02-01	Consulta de páginas web antiguas

9.2 Consultas (dorks) empleadas

- `site:hospitalespascual.com filetype:pdf`
- `site:hospitalespascual.com "@hospitalespascual.com"`
- `"Clínica San Rafael" "Cádiz" PDF`
- `site:hospitalespascual.com intitle:index.of`
- `site:hospitalespascual.com inurl:test`
- `"Neurología" site:hospitalespascual.com`
- `"oncología" site:hospitalespascual.com`
- `"TAC" site:hospitalespascual.com`
- `"resonancia" site:hospitalespascual.com`
- `site:linkedin.com "Hospital San Rafael" Cádiz`
- `"Director Médico" site:hospitalespascual.com`

9.3 Evidencias (índice)

- `evidencias/2026-02-01_ExifTool1.png` - Metadatos de documentos públicos (captura 1)
- `evidencias/2026-02-01_ExifTool2.png` - Metadatos de documentos públicos (captura 2)
- `evidencias/2026-02-01_ExifTool3.png` - Metadatos de documentos públicos (captura 3)
- `evidencias/crtsh_hospitalespascual.png` - Certificados SSL asociados a dominios y subdominios
- `evidencias/dnsdumpster_hospitalespascual.png` - Subdominios y registros DNS pasivos del hospital
- `evidencias/README.md` - Descripción de las evidencias recopiladas
- `evidencias/SpiderFoot_HospitalSanRafael.csv` - Resultados de análisis OSINT automatizado