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 1
- Integrantes: Nerea Candón Ramos(NCR), Inca Vico Prieto(IVP), Asier Gónzalez(AG), Adrián Sánchez(AS).
- Fecha(s) de investigación: 29/01/2026 a 01/02/2026
- Versión: 1.0
- Límite de entrega (a): máximo 6 folios (12 caras) en PDF (si aplica)

1. Resumen ejecutivo

En esta actividad se ha realizado una investigación OSINT pasiva sobre el Hospital San Rafael de Cádiz, utilizando únicamente información que ya estaba disponible públicamente en Internet, sin interactuar con sus sistemas.

El objetivo fue identificar qué datos visibles para cualquiera podían haber ayudado a un atacante a prepararse antes de un incidente de ciberseguridad. Para ello se analizaron la página web del hospital y otras fuentes abiertas, buscando información sobre la organización, el personal, los servicios, los datos de contacto y la estructura interna del centro.

La investigación permitió comprobar que existe una gran cantidad de información accesible, como nombres y cargos de responsables, ubicación exacta, teléfonos, distribución del hospital y descripción detallada de servicios y áreas internas. Aunque esta información es legal y pública, unida puede facilitar engaños, suplantaciones de identidad o correos fraudulentos dirigidos al personal.

Como conclusión, se recomienda revisar el nivel de detalle de la información publicada, limitar la exposición innecesaria y reforzar la concienciación del personal sobre los riesgos de la información pública en Internet.

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).

- A-13: En la sección de Equipo humano, la Clínica nos proporciona una lista con todos los empleados.
- A-01, 02: Se facilita la búsqueda en redes sociales y otras plataformas para su posterior ingeniería social.
- A-14: En la sección "Directorio" se facilita la distribución de las diferentes áres del hospital.
- A-07: En los subdominios se observan servicios expuestos, que puede convertirse en un vector de ataque.

Riesgo global (una frase).

- El riesgo global es alto, debido a la exposición detallada de la estructura organizativa y datos personales del equipo médico, lo que aumenta críticamente la superficie para ataques de ingeniería social dirigidos.

Recomendaciones prioritarias (3-5 bullets).

- **Limitar la exposición de información del personal:** Retirar los listados completos de empleados de la web y concienciar a la plantilla sobre la privacidad en redes sociales para prevenir ataques de ingeniería social.
- **Ocultar detalles de la infraestructura física:** Eliminar planos o directorios detallados de las instalaciones en fuentes públicas para no facilitar el reconocimiento físico.
- **Reducir la superficie de ataque técnica:** Ocultar versiones de tecnologías (WordPress, jQuery) y revisar subdominios expuestos para asegurar que no revelan entornos vulnerables.
- **Sanitización de documentos y metadatos:** Establecer un procedimiento de limpieza de metadatos (usuarios, software) en archivos públicos (PDF) y revisar guías de usuario para no exponer contactos internos.

- **Protección de registros de dominio:** Activar la privacidad en los registros para ocultar datos administrativos y técnicos del dominio.

2. Alcance, supuestos y reglas de compromiso

Alcance. Solo OSINT pasivo sobre la entidad Hospital San Rafael de Cádiz (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):
    - ¿Tiene página web y que puedo sacar de ella?
    - ¿Qué dominios usa la entidad?
    - ¿Existen patrones de email/usuarios visibles públicamente?
    - ¿Existen documentos públicos con metadatos reveladores?
    - ¿Hay menciones de sedes, organigrama o personal?
- Criterios de priorización:
    - Impacto potencial en ingeniería social.
    - Exposición de infraestructura por huella documental/histórica.
    - Exposición de datos personales
- Ventana temporal:
    - Consulta realizada en: [2026-01-29]
    - Evidencias archivadas en: `evidencias/`.

3.2 Identificación de fuentes

Tabla de fuentes:

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
Buscadores	Google	menciones, PDFs, indexación	dorks sin acceder a paneles
Dominios	WHOIS, viewdns	datos de registro	solo consulta pública
DNS pasivo	dnsdumpster, viewdns	subdominios/histórico	sin enumeración activa

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
RRSS	LinkedIn/Facebook/Instagram/TopDoctors	perfiles, roles, nicks	solo contenido público
Metadatos	exiftool	autores, rutas, software	sobre ficheros públicos

3.3 Adquisición (recopilación)

- Consultas realizadas (resumen):
  - Clínica de San Rafael de Cádiz
  - site:hospitalespascual.com filetype:pdf
  - "@hospitalespascual" -site:hospitalespascual.com
- Evidencias:
  - Guardar capturas o PDFs en `evidencias/` con nombres: `YYYY-MM-DD_fuente_tema.ext`
  - Registrar URL (y, cuando sea útil, captura) 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).
  - Continuidad de los patrones previamente vistos (nombres de correos, prefijo de telefono, etc ...)

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	Tipo	Uso concreto	Salida/evidencia
[Herramienta]	[Buscador/DNS/Metadatos/etc.]	[Para qué]	[archivo en evidencias/ o URL]
https://www.google.com/	[Buscador]	Buscador usado para todas las busquedas	No aplica
https://viewdns.info/	[DNS/Dominio]	Ver datos del dominio y dns de la web	evidencias\dominios-subd-huella-dns\dns.png
https://exif.tools/	[Metadatos]	Extraer Metadatos de un archivo	evidencias\huella\2026-01-29_politica.png

5. Resultados (hallazgos)

5.1 Identidades digitales (nicks, perfiles, cuentas)

- A-01

Campo	Contenido
ID	A-01
Categoría	Identidad
Descripción	Busqueda en Google de la web de la "Clínica de San Rafael de Cádiz", y vamos a la sección de "Equipo humano". Comenienza la busqueda por la primera personal que aparece, el Director médico de cirugía general Ignacio Ortiz Acero Equipo humano. Buscando su nombre en Google nos aparece que también trabaja en la calle García Carrera 41, marcado como consultorio privado Consulta privada. En la búsqueda se encuentra una cuenta de Facebook abierta Facebook, en la que se confirma que se trata de la misma persona y gracias a la cual obtenemos información familiar, tanto relaciones personasles y académicas de sus hijos, como información de su esposa Familia.
Evidencia	https://www.doctoralia.es/ignacio-ortiz-acero/cirujano-general/cadiz Consultorio Privado; Facebook https://www.facebook.com/ignacio.ortizacero/ ;Evidencias 01-IOA
Fecha evidencia	2026-01-29
Impacto	La web del Hospital proporciona un catálogo con el nombre, apellidos y fotos de los trabajadores, facilitando la búsqueda. El Facebook abierto permite conocer su vida personal y académica, lo que podría ser utilizado para crear ataques de ingeniería social más creíbles, gracias a los datos concretos.
Riesgo	Alto
Recomendación	Limitar la información de los trabajadores y configurar la privacidad de las cuentas de redes sociales.

- A-02

Campo	Contenido
ID	A-02
Categoría	Identidad

Campo	Contenido
Descripción	Se recopiló información detallada sobre el Dr. Pascual Espinosa a partir de fuentes públicas. En una página web informativa se describe su perfil profesional como médico especialista en Traumatología y Medicina Familiar y Comunitaria, su actividad como traumatólogo y cirujano ortopédico en distintos centros hospitalarios de Cádiz, así como sus áreas de especialización quirúrgica. Durante la investigación OSINT también se localizaron su perfil de LinkedIn, vídeos en redes sociales, artículos publicados en otras páginas web y su registro como profesional sanitario en diversas aseguradoras médicas.
Evidencia	https://www.topdoctors.es/doctor/jose-manuel-pascual-espinosa/ + https://www.linkedin.com/in/jose-manuel-pascual-espinosa-aaa5711b/ + evidencia – captura perfil profesional + evidencia – captura instagram +evidencia – captura linkedin + evidencia – captura TOPDOCTORS
Fecha evidencia	2026-01-29
Impacto	La agregación de información procedente de múltiples fuentes permite a un atacante construir un perfil exhaustivo del médico, facilitando ataques de ingeniería social altamente dirigidos, suplantación de identidad profesional y campañas de phishing personalizadas.
Riesgo	Medio
Recomendación	Centralizar y controlar la información profesional publicada, reducir la exposición innecesaria en redes sociales, revisar la visibilidad de perfiles profesionales y reforzar la formación del personal sanitario frente a ataques de ingeniería social.

- A-03

Campo	Contenido
ID	A-03
Categoría	Identidad
Descripción	A partir de fuentes abiertas se recopiló información sobre Guido Weisman, médico especialista en Traumatología que ejerce en el Hospital San Rafael de Cádiz. Durante la investigación OSINT se localizaron su perfil de LinkedIn, diversas páginas web en las que se hace referencia a su actividad profesional, así como fotografías públicas junto a compañeros de trabajo. Adicionalmente, se identificaron perfiles en redes sociales como Instagram y Facebook, donde se encontraron imágenes de carácter personal que permiten inferir aspectos de su entorno privado.
Evidencia	Foto Universidad · LinkedIn · Instagram · Facebook
Fecha evidencia	2026-01-29
Impacto	La correlación de información profesional y personal procedente de múltiples plataformas permite a un atacante construir un perfil exhaustivo del individuo, facilitando ataques de ingeniería social dirigidos, suplantación de identidad profesional y posibles situaciones de acoso o extorsión.
Riesgo	Alto
Recomendación	Restringir la visibilidad de perfiles personales en redes sociales, separar la identidad profesional de la privada, evitar la publicación de contenido sensible o familiar y reforzar la concienciación sobre los riesgos asociados a la exposición digital.

5.2 Datos de contacto (emails, teléfonos, estructuras)

- A-04

Campo	Contenido
ID	A-04
Categoría	Contacto
Descripción	En la guia de usuario se pueden ver varios datos de contacto
Evidencia	https://www.hospitalespascual.com/wp-content/uploads/2024/03/guia-del-usuario_San-Rafael_Com.pdf + guia1 + guia2
Fecha evidencia	[2026-01-29]
Impacto	Saber vectores de ataque para ingenieria social hospital
Riesgo	Medio
Recomendación	Hacer saber a los empleados que estos datos son públicos

- A-05

Campo	Contenido
ID	A-05
Categoría	Contacto
Descripción	En la guia para el paciente se pueden ver varios telefonos
Evidencia	https://www.hospitalespascual.com/guia-para-el-paciente/ + guia
Fecha evidencia	[2026-01-29]
Impacto	Saber vectores de ataque para ingenieria social
Riesgo	Bajo
Recomendación	Hacer saber a los empleados que estos datos son públicos

5.3 Dominios, subdominios y huella DNS (pasivo)

- A-06

Campo	Contenido
ID	A-06
Categoría	Dominio-DNS
Descripción	Subdominios observados en fuentes pasivas/históricas.
Evidencia	https://viewdns.info/subdomains + Subdominios
Fecha evidencia	[29-01-2026]
Impacto	Permite descubrir servicios expuestos, detectar entornos olvidados, identificar tecnologías, localizar APIs entre otras cosas.
Riesgo	Medio
Recomendación	Reducir lo que "se puede enumerar"; cerrar subdominios innecesarios, aislar entornos, evitar registros DNS de más entre otras.

- A-07

Campo	Contenido
ID	A-07
Categoría	Dominio-DNS
Descripción	Whois permite obtener detalles clave tanto del dominio como de la ip pública asociada.
Evidencia	https://viewdns.info/whois/ + Whois
Fecha evidencia	[29-01-2026]
Impacto	Permite descubrir información sobre el propietario del dominio, fecha de creación, fecha de expiración, etc.
Riesgo	Bajo
Recomendación	No exponer información sensible en Whois activando la privacidad del registrador.

- A-08

Campo	Contenido
ID	A-08
Categoría	Dominio-DNS
Descripción	Obtener la huella DNS del dominio.
Evidencia	https://viewdns.info/dnsreport/ + DNS
Fecha evidencia	[29-01-2026]
Impacto	Permite a un atacante mapear el dominio y que servicios están expuestos.
Riesgo	Medio
Recomendación	Elimina subdominios innecesarios y aísla los entornos dev/staging (VPN o IP allowlist) para reducir la attack surface.

5.4 Huella documental y metadatos (documentos públicos)

- A-09

Campo	Contenido
ID	A-09
Categoría	Documentos-Metadatos
Descripción	Usando la busqueda site:https://www.hospitalespascual.com/ filetype:pdf, se puede obtener un documento pdf con varios metadatos como Autor y herramienta usada
Evidencia	https://www.hospitalespascual.com/wp-content/uploads/2024/09/POLITICA-DE-MEDIOAMBIENTE44.pdf + politica
Fecha evidencia	[2026-01-29]
Impacto	Saber herramientas usadas por la empresa
Riesgo	Bajo
Recomendación	Asegurarse de que no se guarden metadatos de información sensible

- A-10

Campo	Contenido
ID	A-10
Categoría	Huella documental
Descripción	Documento BOJA de un convenio colectivo de hospitalespascual
Evidencia	https://www.juntadeandalucia.es/boja/2018/78/BOJA18-078-00015-7083-01_00134471.pdf + BOJA PDF
Fecha evidencia	[2026-01-29]
Impacto	Información acerca de la empres José Manuel Pascual Pascual S.A (hospitalespascual) social
Riesgo	Bajo
Recomendación	Hacer saber al responble de que este documento es público

5.5 Brechas y filtraciones (consulta pasiva)

- A-11

Campo	Contenido
ID	A-11
Categoría	Brechas
Descripción	Si navegamos por la web de la clínica con la consola de las devtools abierta, podemos observar notificaciones de tecnologías específicas y sus versiones.
Evidencia	https://www.hospitalespascual.com + Wordpress
Fecha evidencia	2026-01-29
Impacto	Permite a un atacante identificar brechas de seguridad en la web de la clínica.
Riesgo	Medio
Recomendación	Evitar la exposición de tecnologías en la medida de lo posible.

- A-12

Campo	Contenido
ID	A-12
Categoría	Brechas
Descripción	Si navegamos por la web de la clínica con la consola de las devtools abierta, podemos observar notificaciones de tecnologías específicas y sus versiones.
Evidencia	https://www.hospitalespascual.com + Jquery
Fecha evidencia	2026-01-29
Impacto	Permite a un atacante identificar brechas de seguridad en la web de la clínica.
Riesgo	Medio
Recomendación	Evitar la exposición de tecnologías en la medida de lo posible.

- A-13

Campo	Contenido
ID	A-13
Categoría	Brechas
Descripción	Busqueda en Google de la web de la "Clínica de San Rafael de Cádiz", y vamos a la sección de "Equipo humano" se puede ver una lista con todos los empleados.
Evidencia	[https://www.hospitalespascual.com/hospital-san-rafael/] + Web
Fecha evidencia	[2026-01-29]
Impacto	Saber todos los empleados que trabajan en el hospital
Riesgo	Alto
Recomendación	Remover la seccion de Equipo humano

- A-14

Campo	Contenido
ID	A-14
Categoría	Brechas
Descripción	Busqueda en Google de la web de la "Clínica de San Rafael de Cádiz", y vamos a la sección de "Directorio" se puede ver información de la distribución de las instalaciones.
Evidencia	[https://www.hospitalespascual.com/hospital-san-rafael/] + Directorio
Fecha evidencia	[2026-01-29]
Impacto	Saber la estructura del edificio
Riesgo	Medio
Recomendación	Remover la seccion de Directorio

6. Resumen de riesgos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-01	Información personal de trabajadores expuesta, facilitando ataques de ingeniería social	Alto	P1	Limitar la información de los trabajadores y configurar la privacidad de las cuentas de redes sociales.
A-02	Información profesional del objetivo encontrada en LinkedIn y páginas web, incluyendo fotos con colegas	Alto	P1	Revisar la información pública en perfiles profesionales y limitar la exposición de datos laborales.
A-03	Información sobre Guido Weisman	Alto	P1	Revisar la información pública en perfiles profesionales y limitar la exposición de datos laborales.
A-04	Información personal en redes sociales (Instagram y Facebook) incluyendo fotos familiares	Medio	P2	Hacer saber a los empleados que estos datos son públicos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-05	En la guia para el paciente se pueden ver varios telefonos	Bajo	P3	Hacer saber a los empleados que estos datos son públicos
A-06	Subdominios observados en fuentes pasivas/históricas.	Medio	P2	Reducir lo que "se puede enumerar"; cerrar subdominios innecesarios, aislar entornos, evitar registros DNS de más entre otras.
A-07	Obtener detalles clave tanto del dominio como de la ip pública asociada.	Bajo	P3	No exponer información sensible en Whois activando la privacidad del registrador.
A-08	Obtener la huella DNS del dominio.	Medio	P2	Elimina subdominios innecesarios y aísla los entornos dev/staging (VPN o IP allowlist) para reducir la attack surface.
A-09	Documento pdf con varios metadatos como autor y herramienta usada	Bajo	P3	Asegurarse de que no se guarden metadatos de información sensible
A-10	Documento BOJA de un convenio colectivo de hospitalespascual	Bajo	P3	Hacer saber al responble de que este documento es público
A-11	Notificaciones de tecnologías específicas y sus versiones. Wordpress	Medio	P2	Evitar la exposición de tecnologías en la medida de lo posible.
A-12	Notificaciones de tecnologías específicas y sus versiones. Jquery	Medio	P2	Evitar la exposición de tecnologías en la medida de lo posible.
A-13	Lista de todos los empleados	Alto	P1	Remover la sección Equipo Humano
A-14	Distribución de las instalaciones.	Medio	P2	Remover la sección de Directorio

7. Conclusiones

- **Exposición crítica de identidades y estructura:** La publicación del organigrama completo y listados de empleados, combinada con la huella digital personal en redes sociales, facilita enormemente la creación de perfiles para ataques de spear phishing altamente creíbles.
- **Transparencia física excesiva:** La disponibilidad pública de directorios y planos del edificio reduce la barrera de entrada para operaciones de seguridad física o reconocimiento presencial, eliminando la necesidad de reconocimiento activo arriesgado.
- **Huella técnica y documental descuidada:** La presencia de subdominios olvidados, versiones de software expuestas y metadatos en documentos PDF revela una falta de higiene digital que podría servir como punto de entrada inicial para comprometer la infraestructura tecnológica.

8. Recomendaciones

Quick wins (0-30 días)

- Limitar la información visible en la sección “Equipo humano” y “Directorio” de la web (A-01, A-13, A-14).
  Responsable: Comunicación / IT
- Configurar la privacidad de las cuentas de redes sociales de los empleados, especialmente de directivos y personal visible públicamente (A-01, A-03).
  Responsable: RRHH / Seguridad

- Retirar o anonimizar metadatos de documentos públicos y PDFs antes de publicarlos en la web (A-09, A-10).
  Responsable: IT / Comunicación
- Avisar al personal sobre la exposición pública de datos de contacto (emails, teléfonos) y la importancia de la concienciación frente a ingeniería social (A-04, A-05).
  Responsable: RRHH / Seguridad
- Evitar que la web muestre versiones de tecnologías y plugins que podrían permitir identificar brechas (A-11, A-12).
  Responsable: IT

Medio plazo (1-3 meses)

- Revisar y centralizar la publicación de información profesional en LinkedIn y otras plataformas; establecer políticas de visibilidad y control de perfiles (A-02, A-03).
  Responsable: RRHH / Comunicación
- Reducir la exposición de subdominios y servicios innecesarios en el DNS; aislar entornos de desarrollo y staging mediante VPN o listas de IP (A-06, A-08).
  Responsable: IT
- Activar privacidad en Whois y evitar exponer datos sensibles del dominio (A-07).
  Responsable: IT
- Establecer procedimientos periódicos de revisión de contenidos publicados, documentos y perfiles profesionales para mantener la información actualizada y segura.
  Responsable: IT / Seguridad / RRHH

Mejora continua

- Implementar un plan de monitorización de menciones y exposición digital de empleados y del hospital para detectar riesgos emergentes.
  Responsable: Seguridad / Comunicación
- Revisiones trimestrales de la superficie de exposición OSINT de la organización.
  Responsable: Seguridad / IT
- Desarrollar un playbook OSINT interno con procedimientos claros de mitigación frente a filtraciones, ingeniería social y exposición de datos.
  Responsable: Seguridad / IT
- Formar continuamente al personal sobre riesgos de seguridad digital, ingeniería social y buenas prácticas en redes sociales y publicación de información.
  Responsable: RRHH / Seguridad

9. Anexos

9.1 Registro de fuentes

Fuente	URL	Fecha acceso	Nota
Web Hospitales Pascual, San Rafael	https://www.hospitalespascual.com/hospital-san-rafael/	2026/01/29	Equipo Humano, Directorio
Doctoralia Ignacio Ortiz	https://www.doctoralia.es/ignacio-ortiz-acero/cirujano-general/cadiz	2026/01/29	Consultorio Privado IOA
Facebook Ignacio Ortiz	https://www.facebook.com/ignacio.ortizacero/	2026/01/29	Red Social

Fuente	URL	Fecha acceso	Nota
LinkedIn Guido Weisman	https://www.linkedin.com/in/guido-weisman-baa92824b/	2026/01/30	Perfil profesional
SegurCaixa Adeslas Guido Weisman	https://www.segurcaixaadeslas.es/cuadromedico/l/traumatologos/cadiz	2026/01/30	Cuadro médico
Facebook Guido Weisman	https://www.facebook.com/guidoweis/?locale=es_LA	2026/01/30	Red Social
Instagram Guido Weisman	https://www.instagram.com/gugaweis/?hl=es	2026/01/30	Red Social
LinkedIn José Manuel Pascual	https://www.linkedin.com/in/jose-manuel-pascual-espinosa-aaa5711b/	2026/01/30	Perfil profesional
Facebook Hospital Pascual	https://www.facebook.com/hospitalespascual/videos/3411228055856310/	2026/01/30	Red Social / Video
TopDoctors José Manuel Pascual	https://www.topdoctors.es/doctor/jose-manuel-pascual-espinosa/	2026/01/30	Consultorio Privado
Web Hospitales Pascual	https://www.hospitalespascual.com/hospital-san-rafael/	2026/01/30	Equipo Humano
Guia de Usuario	https://www.hospitalespascual.com/wp-content/uploads/2024/03/guia-del-usuario_San-Rafael_Com.pdf	2026/01/29	Contactos
Guia para el paciente	https://www.hospitalespascual.com/guia-para-el-paciente/	2026/01/29	Contactos
Politica de medioambiente	https://www.hospitalespascual.com/wp-content/uploads/2024/09/POLITICA-DE-MEDIOAMBIENTE44.pdf	2026/01/29	Metadatos

9.2 Consultas (dorks) empleadas

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

- site:hospitalespascual.com filetype:pdf "San Rafael"
- site:hospitalespascual.com "equipo humano"
- site:linkedin.com "Ignacio Ortiz Acero"
- site:linkedin.com "Guido Weisman"
- site:linkedin.com "José Manuel Pascual Espinosa"
- site:facebook.com "Ignacio Ortiz Acero"
- site:facebook.com "Guido Weisman"
- site:facebook.com "Hospitales Pascual"
- site:instagram.com "gugaweis"
- site:topdoctors.es "José Manuel Pascual Espinosa"
- site:segurcaixaadeslas.es "traumatologos Cádiz"
- "Clínica San Rafael" "Cádiz" "información personal"
- "Clínica San Rafael" "Cádiz" "equipo médico"

9.3 Evidencias (índice)

- evidencias/:
  - brechas-y-filtraciones/
    - 01-Wordpress.png - prueba de que la web usa WordPress y version
    - 02-Jquery.png - prueba de que la web usa Jquery y version
    - 2026-01-29_directorio.png - Información sobre la infraestructura del hospital
  - contacto/
    - 2026-01-29_guia1.png - Información de contacto
    - 2026-01-29_guia2.png - Información de contacto
    - 2026-01-29_guia3.png - Información de contacto
  - dominios-subd-huella-dns/
    - certificadosSSL.png - Información de certificados SSL
    - dns.png - Información de dns
    - subdominios.png - Información de subdominios
    - WHOIS.png - Información general del dominio
  - huella-documental/
    - 2026-01-29_politica.png - Metadatos del pdf
    - BOJA.png - Información interna del hospital
  - identidades-digitales/
    - A-01
      - 2026-01-29_doctoralia - Información del personal
      - 2026-01-29_facebook_familia - Información del personal
      - 2026-01-29_facebook - Información del personal
      - 2026-01-29_web - Información del personal
    - A-02
      - 2026-01-29-aseguradora - Información del personal
      - 2026-01-29-instagram - Información del personal
      - 2026-01-29-linkedin - Información del personal
      - 2026-01-29-TOPDOCTORS - Información del personal
    - A-03
      - 2026-01-29-facebook - Información del personal
      - 2026-01-29-instagram - Información del personal
      - 2026-01-29-instagramm - Información del personal
      - 2026-01-29-linkedin - Información del personal
      - 2026-01-29-SAM - Información del personal