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 2
- Integrantes: [Pablo González Silva], [Carlos Alcina Romero] y [Luis Carlos Romero Navarro]
- Fecha(s) de investigación: [2026-01-26 a 2026-02-01]
- Versión: 1.0
- Límite de entrega (a): máximo 6 folios (12 caras) en PDF (si aplica)

1. Resumen ejecutivo

Durante el periodo 2026-01-26 a 2026-02-01 se realizó una auditoría OSINT pasiva sobre la huella pública asociada al Hospital San Rafael (Cádiz) y su presencia digital vinculada (web corporativa, perfiles y fuentes de terceros ya recolectadas). El objetivo fue identificar información disponible antes del incidente supuesto que facilitase el reconocimiento: estructura de dominios/subdominios, exposición de canales de correo y administración, tecnologías empleadas, publicación de personal/roles y referencias públicas relevantes. Se consultaron fuentes de DNS pasivo/CT logs (p. ej., SecurityTrails/crt.sh), registros públicos (p. ej., RIPE), y contenidos accesibles públicamente (p. ej., web corporativa/directorios). Los hallazgos muestran una combinación de exposición organizativa (roles y nombres) y exposición técnica (subdominios y stack) que reduce el coste de preparación de ataques de phishing/suplantación y ayuda a perfilar infraestructura y proveedores.

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).

- Se observan múltiples subdominios orientados a correo y administración (p. ej., autodiscover, webmail/cpanel/whm, ftp, webdisk, test), identificables por fuentes pasivas; esto facilita el mapeo de superficie y la preparación de campañas de suplantación.
- La configuración DNS/MX publica rutas de correo (p. ej., servidor principal y backup), lo que permite a un atacante adaptar señuelos (phishing/BEC) a los canales reales de la organización.
- El sitio web parece basarse en WordPress y plugins conocidos (p. ej., Elementor/WPML), y se identifica la existencia de panel de administración; conocer el stack reduce el esfuerzo de búsqueda de vulnerabilidades y de ingeniería social técnica.
- Existe un directorio público con nombres y cargos/especialidades de personal (incluyendo roles de dirección), complementable con perfiles profesionales públicos; esto habilita spear phishing altamente dirigido.

- Se hallaron referencias a exposición en brechas de terceros (p. ej., verifications.io) y a información corporativa/registral pública; esto puede alimentar intentos de reutilización de credenciales y pretextos creíbles.

Riesgo global (una frase).

- Medio por la combinación de exposición de identidades/roles y huella técnica (subdominios, correo y tecnologías), que incrementa la probabilidad y efectividad de ataques de ingeniería social y abuso de servicios expuestos.

Recomendaciones prioritarias (3-5 bullets).

- Reducir la exposición de subdominios sensibles: despublicar los no necesarios (p. ej., entornos "test") y restringir el acceso a paneles de administración/correo (WAF, allowlist/VPN, 2FA).
- Minimizar datos personales publicados: revisar el "cuadro médico" y contenidos para limitar detalles no imprescindibles (especialmente roles de dirección) y evitar publicación directa de correos/telefonía cuando no aporte valor.
- Gestionar el riesgo del CMS: inventario de plugins, actualización y hardening de WordPress (2FA, control de accesos, desactivar superficies no usadas, monitorización de vulnerabilidades).
- Implantar monitorización continua de exposición: alertas de CT logs/DNS pasivo, seguimiento de menciones y revisión periódica de brechas que afecten a dominios corporativos.

2. Alcance, supuestos y reglas de compromiso

Alcance. Investigación OSINT estrictamente pasiva sobre la entidad objetivo (Clínica/Hospital San Rafael de Cádiz) y su huella pública asociada: presencia web, información corporativa pública, huella de dominios/subdominios observada por terceros, y perfiles profesionales/páginas públicas relacionadas. Se excluye deliberadamente la investigación individual en profundidad (apartado b) y cualquier verificación técnica activa.

Ventana temporal y supuestos.

- Ventana de consulta: 2026-01-26 a 2026-02-01.
- Los datos reflejan lo que terceros y fuentes públicas mostraban en la fecha de consulta; pueden existir cambios posteriores (alta/baja de subdominios, cambios de proveedor, modificaciones de contenido).
- La presencia de un subdominio o certificado en fuentes pasivas no implica necesariamente que el servicio estuviera accesible en el momento de la investigación.

Fuentes consultadas (OSINT pasivo, 5-10).

- Web corporativa/directorios públicos (p. ej., cuadro médico y páginas informativas): evidencia en Tabla-Trabajadores-Web y Trabajadores-Web (fuente: hospitalespascual.com).
- DNS pasivo / histórico de subdominios: evidencia en 2026-01-26_securitytrails_subdominios (fuente: securitytrails.com).
- Certificate Transparency / CT logs: evidencia en 2026-01-26_crt.sh_subdominios (fuente: crt.sh).

- Registros de red/propiedad IP (WHOIS/RIPE): evidencia en 2026-01-26_whois_duenoip (fuente: RIPE NCC).
- Consultas DNS públicas exportadas (A/NS/MX/SOA): evidencia en 2026-01-26_whois_dns (fuente: exportación de consulta DNS/WHOIS).
- Información tecnológica publicada por tercero/proveedor: evidencia en 2026-02-01_tecnologiaweb_ptg.digital (fuente: ptg.digital).
- Bases de datos/noticias de brechas de terceros (consulta pasiva): evidencia en 2026-02-01_brechaseguridad_verification.io (fuente: verifications.io).
- Fuentes judiciales/registro público (consulta y lectura): evidencia en 2026-02-01_demandashospital_poderjudicial.es (fuente: poderjudicial.es).
- Perfiles profesionales públicos (solo confirmación de rol/posición pública): evidencia en IreneMoyaGarcia y SergioMunozPinero (fuente: linkedin.com).
- Datos corporativos públicos (identificación y contacto publicados): evidencia en 2026-02-01_informacionempresa_rmc.es (fuente: rmc.es).

Regla crítica (no actividad).

- No se han realizado escaneos, enumeración directa de servicios, fingerprinting activo, pruebas de login, ni interacción con formularios.
- No se han lanzado peticiones deliberadas a paneles, webmail, cPanel/WHM u otros endpoints con el objetivo de comprobar disponibilidad o extraer banners.
- En caso de usar herramientas que podrían emplearse activamente, se han usado solo como consulta de datos ya recolectados por terceros (DNS pasivo/CT logs), sin generar tráfico hacia la infraestructura objetivo.

Minimización y privacidad.

- Se evita incluir datos personales innecesarios (p. ej., fecha de nacimiento, teléfonos personales, imágenes de perfil) cuando no aportan al análisis de riesgo.
- Cuando es suficiente para justificar el hallazgo, se prioriza describir roles/funciones sobre identificar a personas concretas.
- Si aparece información de contacto o identificadores personales, se recomienda enmascarado parcial o reducción al mínimo (p. ej., mostrar solo dominio o patrón, no direcciones completas).

3. Metodología (ciclo OSINT)

Esta sección describe el proceso seguido según el ciclo OSINT (planificación, adquisición, procesamiento, análisis y difusión) con un enfoque estrictamente pasivo.

3.1 Planificación y dirección

- Objetivo operativo: identificar información pública que facilite reconocimiento (infraestructura, correo, tecnologías, personal/roles, menciones públicas) y priorizar lo que más reduce el esfuerzo de un atacante.
- Preguntas guía aplicadas:
  - ¿Qué dominios/subdominios y servicios asociados aparecen en fuentes pasivas?
  - ¿Qué canales de contacto/correo se pueden inferir o confirmar de forma pública?

  - ¿Qué tecnologías web se asocian al portal (CMS/plugins/proveedor) según fuentes públicas?
  - ¿Qué información de personal/roles se publica en directorios o perfiles profesionales?
  - ¿Existen referencias públicas relevantes (brechas, demandas, información corporativa) que mejoren la credibilidad de pretextos o indiquen riesgo?
- Criterios de priorización aplicados:
  - Exposición que habilita ingeniería social (roles críticos, contactos, patrones) y phishing/BEC.
  - Exposición técnica que facilita enumeración indirecta (subdominios de administración/correo, entornos de prueba) o acota el stack.
  - Trazabilidad: hallazgos respaldados por evidencia archivada y/o fuentes de terceros reputadas.
- Ventana temporal y trazabilidad:
  - Consulta realizada: 2026-01-26 a 2026-02-01.
  - Evidencias archivadas en `evidencias/` y referenciadas en este informe (p. ej., 2026-01-26_securitytrails_subdominios y 2026-01-26_crt.sh_subdominios).

3.2 Identificación de fuentes

Tabla de fuentes utilizadas (OSINT pasivo):

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
Web corporativa	hospitalespascual.com	directorios públicos, contenidos, estructura informativa	solo lectura, sin interacción (no formularios/login)
DNS pasivo	securitytrails.com	subdominios observados por terceros	consulta sobre datos históricos de terceros
CT logs	crt.sh	CN/SAN de certificados y subdominios	consulta sobre transparencia de certificados
WHOIS/RIPE	ripe.net	asignación de IP, netblocks, entidad asociada	consulta pública, sin contacto directo
Información tecnológica	ptg.digital	referencias públicas sobre desarrollo/stack	lectura de contenido público de terceros
Brechas (terceros)	verifications.io	referencia a exposición de correos/datos	consulta pasiva (sin credenciales)
Registro/judicial	poderjudicial.es	menciones y documentos judiciales públicos	lectura de documento público

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
Perfiles profesionales	linkedin.com	confirmación de rol/posición pública	solo información pública; sin interacción
Información corporativa	rmc.es	datos registrales/identificación pública	consulta/lectura de información pública

3.3 Adquisición (recopilación)

- Consultas representativas (todas pasivas):
  - En CT logs: búsqueda por dominio y comodines para identificar CN/SAN asociados.
  - En DNS pasivo: consulta del dominio principal y revisión de subdominios relacionados con correo/administración.
  - En web corporativa: revisión del directorio público (cuadro médico) y páginas institucionales.
  - En registro/judicial: búsqueda/lectura de documentos públicos asociados a la entidad.
  - En fuentes de brechas: verificación de aparición del dominio en referencia pública.
- Evidencias y trazabilidad:
  - Exportaciones y notas archivadas en `evidencias/` con prefijo de fecha y dominio de la fuente (p. ej., 2026-02-01_demandashospital_poderjudicial.es).
  - Para directorios y listados, se guardaron extracciones en texto/tabla (p. ej., Trabajadores-Web).

3.4 Procesamiento y organización

- Normalización:
  - Deduplicación de subdominios y agrupación por función (correo, administración, pruebas).
  - Agrupación de hallazgos por categoría del informe (Identidad/Contacto/Dominio-DNS/Tecnologías/Brechas).
- Control de calidad:
  - Se priorizaron fuentes de terceros reputadas (CT logs, DNS pasivo) y documentos/URLs públicas.
  - Se anotó la fecha de consulta y se asumió posible variación temporal (p. ej., un subdominio puede aparecer en CT logs aunque ya no esté activo).
  - Se evitó "confirmación activa" (no se verificó disponibilidad de servicios mediante acceso directo a paneles).

3.5 Análisis e interpretación

- Correlaciones utilizadas para generar "inteligencia":
  - Subdominios orientados a correo (p. ej., autodiscover, mail, webmail) + rutas MX publicadas habilitan señuelos realistas y campañas BEC/phishing más creíbles.

  - Subdominios de administración/operación (p. ej., cpanel/whm) + conocimiento del stack (WordPress/plugins) reduce el coste de preparación de ataques técnicos y de suplantación.
  - Directorio público de personal/roles + perfiles profesionales públicos permite selección de objetivos y personalización de mensajes (spear phishing).
  - Referencias a brechas de terceros incrementa probabilidad de reutilización de credenciales y necesidad de controles (2FA/rotación).
- Valoración de riesgo (escala simple):
  - Alto: facilita suplantación o preparación de ataques con alta probabilidad/impacto.
  - Medio: información útil pero requiere pasos adicionales o tiene incertidumbre temporal.
  - Bajo: información genérica sin explotación directa.

3.6 Difusión

- Destinatarios: responsables técnicos (IT/Seguridad) y responsables no técnicos (Dirección/Comunicación) para priorizar mitigaciones y concienciación.
- Entregables: informe con hallazgos verificables y evidencia asociada en `evidencias/`, orientado a acciones (quick wins y medidas estructurales).

4. Herramientas utilizadas

Herramienta	Tipo	Uso concreto	Salida/evidencia
SecurityTrails	DNS pasivo	Identificación de subdominios observados por terceros	2026-01-26_securitytrails_subdominios
crt.sh	CT logs	Identificación de CN/SAN y subdominios vía transparencia de certificados	2026-01-26_crt.sh_subdominios
RIPE NCC	WHOIS/RDAP	Asociación de IP/bloques y entidad/proveedor (consulta pública)	2026-01-26_whois_duenoip
Consulta DNS (export)	DNS	Revisión de registros A/NS/MX/SOA publicados	2026-01-26_whois_dns
Web corporativa hospitalespascual.com	Web	Extracción del directorio público (cuadro médico) y datos de roles	Tabla-Trabajadores-Web
Web corporativa hospitalespascual.com	Web	Extracción en bruto del listado (para trazabilidad)	Trabajadores-Web

Herramienta	Tipo	Uso concreto	Salida/evidencia
ptg.digital	Fuente de terceros	Referencias públicas sobre tecnologías/stack y desarrollo	2026-02-01_tecnologiaweb_ptg.digital
verifications.io	Brechas (terceros)	Referencia pública de brecha citada para valorar riesgo de exposición	2026-02-01_brechaseguridad_verification.io
poderjudicial.es	Registro/judicial	Lectura de documento público relacionado (contexto reputacional/organizativo)	2026-02-01_demandashospital_poderjudici
rmc.es	Información corporativa	Consulta de información pública de la entidad (identificación/contacto)	2026-02-01_informacionempresa_rmc.es
LinkedIn	RRSS (público)	Confirmación de rol/posición pública (sin interacción)	IreneMoyaGarcia
LinkedIn	RRSS (público)	Confirmación de rol/posición pública (sin interacción)	SergioMunozPinero

5. Resultados (hallazgos)

Campo	Contenido
ID	A-01
Categoría	Identidad
Descripción	La entidad publica un directorio de profesionales (cuadro médico) con nombres, especialidades y, en algunos casos, roles de responsabilidad visibles públicamente.
Evidencia	Fuente: hospitalespascual.com + Tabla-Trabajadores-Web y Trabajadores-Web.
Fecha evidencia	2026-02-01
Impacto	Facilita la selección de objetivos y la personalización de mensajes (spear phishing) por rol/especialidad; reduce el coste de reconocimiento organizativo.
Riesgo	Alto

Campo	Contenido
Recomendación	Minimizar detalles no imprescindibles (p. ej., evitar resaltar cargos directivos), revisar qué campos se publican y aplicar medidas anti-scraping/monitorización de exposición.

Campo	Contenido
ID	A-02
Categoría	Identidad / RRSS
Descripción	Existen perfiles profesionales públicos de personal con roles administrativos/gestión asociados a la organización, que permiten construir pretextos verosímiles.
Evidencia	Fuente: linkedin.com + IreneMoyaGarcia y SergioMunozPinero.
Fecha evidencia	2026-02-01
Impacto	Aumenta la efectividad de ataques de suplantación dirigidos a áreas administrativas (facturación/proveedores/RRHH), especialmente por teléfono o correo (BEC).
Riesgo	Medio
Recomendación	Guía de “higiene” de perfiles públicos para roles críticos, concienciación anti-phishing/BEC y verificación fuera de banda para solicitudes sensibles.

5.1 Identidades digitales (nicks, perfiles, cuentas)

- A-01
- A-02

5.2 Datos de contacto (emails, teléfonos, estructuras)

Campo	Contenido
ID	A-03
Categoría	Contacto
Descripción	Los registros DNS publicados incluyen servidores de correo (MX) y nombres asociados a correo/autodiscover, visibles sin interacción con la infraestructura (solo lectura de registros).
Evidencia	Fuente: exportación de consulta DNS/WHOIS + 2026-01-26_whois_dns.

Campo	Contenido
Fecha evidencia	2026-01-26
Impacto	Permite a un atacante alinear señuelos con el canal real (p. ej., “problemas de buzón/autodiscover”) y orientar campañas de phishing/BEC.
Riesgo	Medio
Recomendación	Endurecer el correo (SPF/DKIM/DMARC), 2FA en cuentas y procedimientos de verificación para cambios de cuenta bancaria/solicitudes urgentes.

Campo	Contenido
ID	A-04
Categoría	Contacto
Descripción	Se localizan datos de contacto corporativos (web, teléfonos y correo corporativo) en fuentes públicas de información empresarial.
Evidencia	Fuente: rmc.es + 2026-02-01_informacionempresa_rmc.es.
Fecha evidencia	2026-02-01
Impacto	Facilita pretextos creíbles (soporte/proveedores) y ataques de ingeniería social telefónica hacia centralita/administración.
Riesgo	Medio
Recomendación	Publicar solo canales necesarios, aplicar guiones de verificación para llamadas, y usar alias de contacto controlados (no buzones personales) donde sea posible.

5.3 Dominios, subdominios y huella DNS (pasivo)

Campo	Contenido
ID	A-05
Categoría	Dominio-DNS
Descripción	Fuentes de DNS pasivo listan múltiples subdominios relacionados con administración y correo (p. ej., cpanel/whm, webmail, ftp, autodiscover, test), lo que sugiere una superficie ampliada y potencialmente heterogénea.

Campo	Contenido
Evidencia	Fuente: securitytrails.com + 2026-01-26_securitytrails_subdominios.
Fecha evidencia	2026-01-26
Impacto	Reduce el esfuerzo de reconocimiento técnico y permite preparar campañas de suplantación más específicas (menciones a “webmail”, “cpanel”, etc.).
Riesgo	Alto
Recomendación	Revisar necesidad de cada subdominio (especialmente entornos de prueba), aplicar restricciones de acceso (WAF/VPN/allowlist) y monitorizar exposición (CT/DNS pasivo).

Campo	Contenido
ID	A-06
Categoría	Dominio-DNS
Descripción	Los CT logs y la información pública de asignación IP permiten inferir infraestructura y terceros asociados (hostnames/certificados y rango IP/proveedor), sin interacción directa con servicios.
Evidencia	Fuente: crt.sh + 2026-01-26_crt.sh_subdominios; fuente: RIPE NCC + 2026-01-26_whois_duenoip.
Fecha evidencia	2026-01-26
Impacto	Permite perfilar proveedores/terceros y orientar ataques a supply chain o campañas que mencionen servicios concretos observados en certificados.
Riesgo	Medio
Recomendación	Reducir exposición de hostnames innecesarios en certificados, separar entornos, y aplicar hardening/monitorización en servicios expuestos.

5.4 Huella documental y metadatos (documentos públicos)

Campo	Contenido
ID	A-07
Categoría	Documentos-Metadatos

Campo	Contenido
Descripción	Un proveedor/tercero publica información sobre la tecnología/plataforma utilizada (p. ej., CMS y complementos), lo que contribuye al fingerprinting pasivo del stack.
Evidencia	Fuente: ptg.digital + 2026-02-01_tecnologiaweb_ptg.digital.
Fecha evidencia	2026-02-01
Impacto	Reduce el espacio de búsqueda de vulnerabilidades y facilita pretextos técnicos (p. ej., "actualización de WordPress/plugin").
Riesgo	Medio
Recomendación	Mantener inventario de CMS/plugins, actualizar con cadencia, y limitar divulgación innecesaria del stack cuando no aporte valor.

Campo	Contenido
ID	A-08
Categoría	Documentos-Metadatos
Descripción	Existen documentos públicos judiciales/relacionados accesibles vía fuentes oficiales, que pueden ser usados para pretextos reputacionales o de urgencia (ingeniería social).
Evidencia	Fuente: poderjudicial.es + 2026-02-01_demandashospital_poderjudicial.es.
Fecha evidencia	2026-02-01
Impacto	Facilita campañas de suplantación con contexto real (p. ej., "documentación legal pendiente"), aumentando credibilidad y urgencia.
Riesgo	Bajo
Recomendación	Procedimientos de verificación para comunicaciones "legales/urgentes" y canal único controlado para recepción de notificaciones.

5.5 Brechas y filtraciones (consulta pasiva)

Campo	Contenido
ID	A-09

Campo	Contenido
Categoría	Brechas
Descripción	Se referencia una brecha de terceros (verifications.io, 2019) con exposición masiva de correos y datos asociados, potencialmente incluyendo usuarios de dominios relacionados.
Evidencia	Fuente: verifications.io + 2026-02-01_brechaseguridad_verification.io.
Fecha evidencia	2026-02-01
Impacto	Incrementa probabilidad de reutilización de credenciales y facilita campañas de phishing basadas en datos filtrados (sin necesidad de explotar sistemas).
Riesgo	Medio
Recomendación	Forzar 2FA, rotación de credenciales expuestas, revisión de dominios/cuentas afectadas y concienciación específica (phishing post-brecha).

6. Resumen de riesgos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-05	Subdominios de correo/administración visibles en fuentes pasivas	Alto	P1	Reducir exposición (cerrar "test"), restringir paneles (WAF/VPN/2FA) y monitorizar CT/DNS pasivo
A-01	Directorio público con personal/roles (facilita spear phishing)	Alto	P1	Minimizar datos publicados y reforzar concienciación para roles críticos
A-03	Registros MX/correo publicados (facilita BEC/phishing)	Medio	P2	Implementar/ajustar SPF/DKIM/DMARC y 2FA; procedimientos anti-BEC

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-06	Fingerprinting pasivo por CT logs + proveedor/IP	Medio	P2	Revisar hostnames en certificados, segmentación y hardening de servicios
A-02	Perfiles profesionales públicos de roles administrativos	Medio	P2	Guía de exposición en RRSS + verificación fuera de banda
A-04	Datos corporativos públicos de contacto	Medio	P3	Estandarizar canales, scripts de verificación y evitar buzones personales
A-07	Tecnología/stack publicada por terceros	Medio	P3	Gestión de vulnerabilidades en CMS/plugins y reducción de divulgación
A-09	Referencia a brecha de terceros (riesgo de reutilización)	Medio	P3	2FA + rotación/monitorización de credenciales y campañas de concienciación
A-08	Documentos públicos judiciales (pretextos reputacionales)	Bajo	P3	Procedimientos de verificación y canal único de comunicaciones legales

7. Conclusiones

- La huella pública combinó exposición organizativa (roles y nombres en directorios) y exposición técnica (subdominios, correo y stack), reduciendo significativamente el esfuerzo de reconocimiento previo a un incidente.
- La presencia de subdominios orientados a administración/correo y la publicación de información de enrutamiento de email (MX/autodiscover) elevan el riesgo de campañas BEC/phishing y suplantación con señuelos realistas.
- La información "pasiva" de terceros (CT logs/DNS pasivo) y publicaciones externas sobre el stack permiten perfilar proveedores y tecnologías sin interactuar con

la infraestructura, lo que incrementa la probabilidad de ataques oportunistas y dirigidos.
- Referencias públicas (información corporativa, documentos oficiales) pueden convertirse en pretextos de alta credibilidad; la mitigación requiere procesos de verificación y concienciación, no solo controles técnicos.
- La prioridad operativa es reducir superficie innecesaria y reforzar controles de identidad (2FA/DMARC/procedimientos anti-BEC), ya que gran parte del valor para un atacante proviene de ingeniería social basada en información pública.

8. Recomendaciones

Quick wins (0-30 días)

- Revisar y depurar subdominios: despublicar/retirar los no necesarios (p. ej., entornos de prueba) y restringir acceso a paneles de administración/correo con VPN/allowlist + 2FA (Responsable sugerido: IT/Seguridad).
- Reducir exposición del directorio público: revisar "cuadro médico" para limitar detalles no imprescindibles (especialmente cargos/roles directivos) y evitar patrones explotables para spear phishing (Responsable sugerido: Comunicación + RRHH + Dirección).
- Publicar y aplicar un procedimiento anti-BEC: verificación fuera de banda para cambios de cuenta bancaria, facturas urgentes y "solicitudes de dirección/proveedores" (Responsable sugerido: Administración/Finanzas + Seguridad).
- Acciones post-brecha (terceros): forzar 2FA en cuentas, revisar reutilización de contraseñas, y comunicar una alerta interna sobre phishing "post-filtración" (Responsable sugerido: IT/Seguridad + RRHH).
- Guía rápida para perfiles públicos: recomendaciones mínimas para personal en roles críticos (qué no publicar, cómo reducir exposición, cómo validar solicitudes) (Responsable sugerido: RRHH + Comunicación).

Medio plazo (1-3 meses)

- Gestión de vulnerabilidades del portal/CMS: inventario de plugins/temas, actualización con cadencia, mínimos privilegios, backups probados y WAF delante del sitio (Responsable sugerido: IT/Seguridad).
- Política de publicación y revisión: establecer un flujo de aprobación para contenidos públicos (directorios, PDFs, notas corporativas) con checklist de privacidad/seguridad (Responsable sugerido: Comunicación + Legal + Seguridad).
- Formación dirigida a roles críticos (Administración/Finanzas/RRHH/Recepción): phishing/BEC, validación de identidad, y manejo de urgencias/reclamaciones (Responsable sugerido: RRHH + Seguridad).
- Monitorización de exposición: alertas de CT logs y cambios de DNS pasivo; revisión mensual de nuevos subdominios y certificados emitidos (Responsable sugerido: Seguridad).
- Gestión de terceros/proveedores: alinear acuerdos y prácticas para evitar divulgación innecesaria del stack/infra (p. ej., en casos/portfolio), y exigir medidas mínimas (MFA, hardening, notificación) (Responsable sugerido: IT + Compras/Legal + Seguridad).

Mejora continua

- Revisión OSINT trimestral (pasiva) con checklist: subdominios/CT, menciones, brechas citadas, exposición de personal/roles y actualización del registro de evidencias (Responsable sugerido: Seguridad).
- Programa continuo de concienciación: cápsulas cortas + recordatorios anti-phishing/BEC y simulaciones periódicas focalizadas en áreas expuestas (Responsable sugerido: RRHH + Seguridad).
- Playbook de respuesta a suplantación/BEC: canales de reporte, verificación rápida, bloqueo/alerta y comunicación interna/externa (Responsable sugerido: Seguridad + Comunicación + Dirección).
- Métricas y control: seguimiento de DMARC, tasas de 2FA, incidencias de suplantación y reducción de superficie (subdominios retirados/paneles restringidos) (Responsable sugerido: IT/Seguridad).

9. Anexos

9.1 Registro de fuentes

Fuente	URL	Fecha acceso	Nota
Web corporativa	https://www.hospitalespasenia.com/	2026-02-01	Directorios públicos y contenido informativo; evidencias en Tabla-Trabajadores-Web y Trabajadores-Web.
DNS pasivo (SecurityTrails)	https://securitytrails.com/	2026-01-26	Subdominios históricos observados por terceros; evidencia en 2026-01-26_securitytrails_subdominios.
CT logs (crt.sh)	https://crt.sh/	2026-01-26	CN/SAN de certificados asociados al dominio; evidencia en 2026-01-26_crt.sh_subdominios.
WHOIS/RDAP (RIPE NCC)	https://www.ripe.net/	2026-01-26	Asignación de rango IP/proveedor; evidencia en 2026-01-26_whois_duenoip.
Exportación local de consulta DNS/WHOIS	—	2026-01-26	Registros A/NS/MX/SOA archivados; evidencia en 2026-01-26_whois_dns.

Fuente	URL	Fecha acceso	Nota
Información tecnológica (tercero)	https://www.ptg.digital/	2026-02-01	Referencias públicas sobre stack/plataforma; evidencia en 2026-02-01_tecnologiaweb_ptg.digital.
Brechas (terceros)	https://verifications.io/	2026-02-01	Referencia pública de brecha; evidencia en 2026-02-01_brechaseguridad_verification.io
Fuente oficial/judicial	https://www.poderjudicial.es/	2026-02-01	Documento público consultado; evidencia en 2026-02-01_demandashospital_poderjudici
Información corporativa (tercero)	https://rmc.es/	2026-02-01	Datos de identificación/contacto publicados; evidencia en 2026-02-01_informacionempresa_rmc.es.
Perfiles profesionales públicos	https://www.linkedin.com/	2026-02-01	Confirmación de rol/posición pública; evidencias en IreneMoyaGarcia y SergioMunozPinero.

9.2 Consultas (dorks) empleadas

Consultas representativas (todas pasivas y reproducibles en buscadores/fuentes OSINT; no implican interacción con paneles ni pruebas de acceso):

- `site:hospitalespascual.com`
- `site:hospitalespascual.com filetype:pdf`
- `site:hospitalespascual.com filetype:doc OR filetype:docx OR filetype:xls OR filetype:xlsx`
- `site:hospitalespascual.com "@hospitalespascual.com"`
- `site:hospitalespascual.com "correo" OR "email" OR "contacto"`
- `site:hospitalespascual.com "cuadro médico" OR "especialidad" OR "unidad"`
- `site:hospitalespascual.com inurl:wp-content OR inurl:wp-includes`
- `"Hospital San Rafael" "Cádiz" hospitalespascual`
- `"Clínica San Rafael" Cádiz "Hospitales Pascual"`
- `site:ptg.digital hospitalespascual`
- `site:rmc.es hospitalespascual OR "Hospitales Pascual"`
- `site:poderjudicial.es "Hospital San Rafael" OR hospitalespascual`

9.3 Evidencias (índice)

- evidencias/README — Nota/índice interno del equipo.
- 2026-01-26_crt.sh_subdominios — Subdominios observados en CT logs (crt.sh).
- 2026-01-26_securitytrails_subdominios — Subdominios observados por DNS pasivo (SecurityTrails).
- 2026-01-26_whois_dns — Exportación de registros DNS (A/NS/MX/SOA).
- 2026-01-26_whois_duenoip — Información de asignación de IP/rango (WHOIS/RIPE).
- 2026-02-01_tecnologiaweb_ptg.digital — Referencias públicas sobre tecnología/stack (tercero).
- 2026-02-01_informacionempresa_rmc.es — Información corporativa pública (tercero).
- 2026-02-01_demandashospital_poderjudicial.es — Documento/nota de fuente oficial (poderjudicial.es).
- 2026-02-01_brechaseguridad_verification.io — Referencia a brecha (verifications.io).
- 2026-02-01_infohospital_googledorks — Capturas/resultado de consultas pasivas (dorks) archivadas.
- `evidencias/trabajadores/`:
  - Tabla-Trabajadores-Web — Tabla del directorio público (cuadro médico).
  - Trabajadores-Web — Extracción en bruto del listado (trazabilidad).
  - IreneMoyaGarcia — Perfil público (confirmación de rol).
  - JoseManuelPascual — Perfil/nota pública (contexto de rol).
  - SergioMunozPinero — Perfil público (confirmación de rol).