Informe de Auditoría de Exposición Digital

Revisión externa, pasiva y documentada de la huella digital pública

Cliente	Cliente Ejemplo, S.L. (anonimizado)
Dominio principal	ejemplo-cliente.es
Dominios secundarios	ejemplo-cliente.com · ejemplo-clientte.es
Ventana de análisis	16 – 20 de mayo de 2026
Referencia	AED-EJEMPLO-001
Versión	1.0
Realizado por	Dragos C.I. Andrei

VERSIÓN ANONIMIZADA con fines de portafolio. El cliente real, sus dominios, identificadores y direcciones IP han sido sustituidos por valores ficticios. La metodología, la estructura de hallazgos y las recomendaciones reproducen un caso real de auditoría.

Aviso de alcance y limitaciones

Esta auditoría es una revisión **externa, pasiva y no intrusiva** de la huella digital pública del cliente. Toda la información analizada es de acceso público y se ha obtenido sin acceder a sistemas, credenciales o redes internas, y sin realizar pruebas de intrusión, fuerza bruta ni explotación de vulnerabilidades.

Este informe **no es** un test de intrusión, una auditoría de cumplimiento normativo (RGPD, LOPDGDD, ENS, ISO 27001) ni un dictamen pericial. Es una **revisión técnica orientada a la toma de decisiones**, defendible en su metodología y trazable en sus evidencias.

Las evidencias recogidas se conservan con sus hashes SHA-256 durante **90 días** desde la entrega de este informe. Determinadas verificaciones (DKIM, exposición de credenciales por cuenta, análisis del servicio Nextcloud, titularidad de dominios .es) requieren colaboración del cliente o acceso autorizado, y se documentan como tales.

1. Resumen ejecutivo

Esta sección está pensada para leerse en 3-4 minutos por una persona sin perfil técnico.

Conclusión general

La presencia digital de Cliente Ejemplo presenta un perfil **mixto**, característico de una pyme que recibió en su momento un trabajo técnico competente pero que no ha tenido mantenimiento continuo coordinado. Conviven elementos muy bien resueltos (cifrado web sobresaliente, infraestructura de correo profesional, registro defensivo de dominios) con carencias relevantes que conviene atender.

Se identifican **dos asuntos críticos**: la medición analítica de la web está completamente inactiva desde, presumiblemente, la migración a Google Analytics 4 de 2023, por lo que el negocio decide sin datos; y un sistema de seguimiento de marketing (Mailchimp) se carga sin el consentimiento previo del usuario, con riesgo de incumplimiento de la normativa española de cookies y protección de datos.

No se han detectado indicios de incidente activo, suplantación de marca en curso ni compromiso de sistemas. La superficie digital es compacta y ordenada.

Distribución de hallazgos

Criticidad	Nº	Significado
Crítico	2	Atender en menos de 7 días
Alto	4	Atender en menos de 30 días
Medio	4	Planificar en los próximos 3 meses
Bajo / Informativo	3	Mejora recomendable sin urgencia
Aspectos correctos	9	Sin acción requerida

Los cinco puntos que más importan

1. La analítica web no funciona (Crítico). Google Analytics está instalado con código obsoleto incompatible con el identificador moderno. La web no registra visitas, fuentes ni conversiones.

2. Seguimiento de marketing sin consentimiento (Crítico). El sistema de Mailchimp se activa antes de que el usuario acepte cookies, lo que puede constituir infracción de LSSI y RGPD.

3. Plugin desactualizado con historial de vulnerabilidades (Alto). Slider Revolution está dos años obsoleto, en una tienda que procesa pagos y datos de clientes.

4. Sistema documental sin gobernanza clara (Alto). Existe un Nextcloud en archivo.ejemplo-cliente.es cuya titularidad y mantenimiento no están documentados.

5. Cuenta de proveedor externo con acceso activo (Alto). Se detecta una cuenta de agencia con actividad más reciente que la del propio cliente.

Recomendación de prioridades para los próximos 30 días

1. **Reparar la medición de Google Analytics** (1 hora, 0 €). Recuperar visibilidad del negocio digital.
2. **Configurar el bloqueo previo de cookies de marketing** (1-2 horas, coste bajo). Reducir el riesgo legal.
3. **Verificar y actualizar Slider Revolution y el tema Bridge** (2-4 horas). Cerrar el principal vector técnico.
4. **Inventariar formalmente los activos digitales**. Saber qué se tiene, quién lo controla y cuándo vence.

2. Metodología y capas analizadas

Se han revisado siete capas de la presencia digital, correlacionando hallazgos entre ellas:

Capa	Qué se revisa
1. Dominio y DNS	Titularidad, vencimientos, resolución de nombres
2. Correo	Autenticación SPF, DKIM, DMARC
3. Web pública	Cabeceras, certificado, tecnología, información expuesta
4. Credenciales	Exposición en filtraciones públicas
5. Suplantación y marca	Dominios similares, certificados, activos no inventariados
6. Analítica	Medición, cookies y consentimiento
7. Continuidad y propiedad	Control de activos, servicios huérfanos, puntos de fallo

Herramientas: whois, dig (BIND 9), curl, openssl, testssl.sh v3.2, dnstwist, consultas a Certificate Transparency (crt.sh), análisis de HTML mediante grep/regex. Consultas desde IP residencial en España, identificándose con User-Agent de auditoría donde aplicaba.

Nota metodológica. Cuando una herramienta devolvía resultados vacíos se aplicó verificación de control (positive control test) para distinguir entre ausencia confirmada y fallo de herramienta. Las limitaciones (servicio crt.sh intermitente, restricciones WHOIS en dominios .es) se documentan en sus hallazgos.

3. Hallazgos detallados por capa

Capa 1 — Dominio y DNS

ALTO **1.1 Vencimiento próximo del dominio principal**

Qué se observó. El dominio ejemplo-cliente.com (registrado en junio de 2000, 26 años) expira el 23 de junio de 2026, a 38 días del análisis. Debe verificarse igual el dominio principal .es.

Por qué importa. Un dominio con 26 años de historia y reputación de marca con DOP es un activo crítico. Su pérdida implicaría caída de web y correo, y posible registro por terceros para suplantación o reventa.

Aspecto positivo. Tiene activado clientTransferProhibited, que impide la transferencia no autorizada.

Qué hacer. Renovar por 5 años; verificar que el contacto administrativo es del cliente, no de un tercero; mantener el bloqueo de transferencia. **Esfuerzo:** 1 h · ~10-15 €/año.

Evidencia: whois-cliente.txt · SHA-256 9724cf91…dae4c5

MEDIO **1.2 DNSSEC no activado**

Qué se observó. El dominio no tiene firmas DNSSEC (estado unsigned).

Por qué importa. DNSSEC protege frente a manipulación de respuestas DNS en tránsito. Su ausencia es común pero su activación es recomendable para una marca con valor.

Qué hacer. Solicitar al proveedor DNS la activación (habitualmente gratuita). **Esfuerzo:** 30 min · 0 €.

Aspectos correctos verificados en Capa 1

• SPF con política estricta (-all): rechaza correos de servidores no autorizados.
• Tres servidores DNS redundantes.
• IPv6 activado (infraestructura moderna).

Evidencia: dig-cliente.txt · SHA-256 543cc3fb…9171f2

Capa 2 — Correo corporativo

ALTO **2.1 Política DMARC publicada pero no aplicada**

Qué se observó. El dominio publica DMARC con política `p=none`, que indica al receptor no actuar ante fallos de autenticación, y sin dirección de reporte (rua).

```
v=DMARC1; p=none
```

Por qué importa. Pese al SPF estricto, DMARC le dice al mundo que no haga nada cuando un correo falle la verificación. Un atacante puede suplantar @ejemplo-cliente.es y alcanzar la bandeja de clientes y proveedores; el cliente ni se entera de los intentos. Relevante para una marca con DOP.

Qué hacer. Configurar buzón de reportes; pasar a `v=DMARC1; p=none; rua=mailto:dmarc-reports@…; pct=100`; tras 2-4 semanas escalar a quarantine y luego reject. **Esfuerzo:** 1 h + observación · 0 €.

Evidencia: dmarc-cliente.txt · SHA-256 a6fb3826…31510a

MEDIO **2.2 Configuración DKIM no verificable externamente**

Qué se observó. Los 10 selectores DKIM comunes no devuelven registro. DKIM no usa selectores estándar, por lo que no puede confirmarse sin acceso del cliente.

Por qué importa. DKIM es la tercera pata de la autenticación de correo. Su ausencia reduce la eficacia de DMARC y puede afectar a la entregabilidad en Gmail/Outlook.

Qué hacer. Solicitar al proveedor confirmación del selector activo o su activación. **Esfuerzo:** 30 min · 0 €.

Evidencia: dkim-cliente.txt · SHA-256 b2bd5384…43b71

Capa 3 — Web pública

Hallazgo 3.0 (informativo): la web responde en ejemplo-cliente.es; el .com redirige mediante 301 permanente, forma técnicamente correcta de gestionar dominios paralelos.

ALTO **3.1 Ausencia de cabeceras HTTP de seguridad**

Qué se observó. El servidor responde sin ninguna cabecera de seguridad recomendada por OWASP: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy ni Permissions-Policy.

Por qué importa. Cada una protege al visitante frente a un ataque distinto. Sin CSP, una vulnerabilidad en cualquier plugin facilita inyección de scripts, incluido el robo de datos en la página de pago (Magecart), riesgo real al procesar pagos. Sin HSTS, posible forzado de conexión insegura. Sin X-Frame-Options, clickjacking.

Contraste. El propio Nextcloud del cliente (Hallazgo 5.3) tiene estas cabeceras impecables: la organización sabe hacerlo, solo falta replicarlo en WordPress.

Qué hacer. Configurar cabeceras vía plugin (Wordfence, Really Simple Security Pro) o en Apache; validar en securityheaders.com (objetivo B o superior). **Esfuerzo:** 30-60 min · 0 €.

Evidencia: headers-cliente-es.txt · SHA-256 79df303a…f86f63b3

POSITIVO **3.2 Certificado TLS válido y correcto**

Certificado DV de CA comercial, válido 11/10/2025 – 25/10/2026, SHA-256 con RSA 2048, cubre el dominio y su www, con tres SCTs de Certificate Transparency. Adecuado al contexto. *Optimización opcional:* migrar a Let's Encrypt (gratuito, equivalente).

Evidencia: tls-cliente.txt · SHA-256 4f08c1ac…51b4f

POSITIVO **3.3 Configuración TLS sobresaliente — A+ (93/100)**

Análisis con testssl.sh: protocolos obsoletos deshabilitados, TLS 1.2 y 1.3 activos, Forward Secrecy completa, sin vulnerabilidad a Heartbleed, ROBOT, POODLE, BEAST, CRIME, FREAK, DROWN, SWEET32 ni LOGJAM.

Observaciones menores. Ofrece cifrados CBC antiguos (LUCKY13 teórico, difícil de explotar) y compresión gzip (BREACH teórico, no aplicable). OCSP stapling no activado. Mejoras opcionales sin urgencia.

Evidencia: testssl-cliente.txt · SHA-256 8b031538…d72a1

ALTO **3.4 Versiones expuestas; Slider Revolution desactualizado**

Qué se observó. La web expone versiones vía metaetiquetas generator: WordPress 6.9.4 (al día), WooCommerce 10.7.0 (al día), WPML 4.9.2.1, y **Slider Revolution 6.7.51 — versión actual 7.0.13, dos años obsoleto**. Se identificaron 15 plugins, incluyendo pasarela Stripe, Mailchimp, Yoast y Really Simple Security.

Por qué importa. Slider Revolution tiene historial de vulnerabilidades críticas (CVE-2014-9734 y posteriores). Una versión de hace dos años, probablemente sin licencia activa, no recibe parches. Sugiere licencia del tema premium Bridge no renovada. La exposición de versiones facilita el reconocimiento automatizado. El contexto de tienda con datos de clientes eleva las implicaciones RGPD.

Qué hacer. Verificar y actualizar/sustituir Slider Revolution; revisar licencia de Bridge y WPBakery; suprimir metaetiquetas generator; política de actualización semanal con backup; valorar WAF gestionado. **Esfuerzo:** 3-5 h + recurrente · ~25-85 USD licencias.

Evidencia: hallazgo-generator.txt (2d11daf3…3273d) · hallazgo-plugins.txt (b85cff65…c67374)

MEDIO **3.5 Hardening de archivos sensibles inconsistente**

Qué se observó. El acceso a readme.txt está bloqueado para revslider y js_composer pero permitido para contact-form-7 y woocommerce. Hardening selectivo, no sistemático.

Qué hacer. Regla universal que bloquee readme/changelog/license de todos los plugins y temas (ver Anexo Técnico A). **Esfuerzo:** 15 min · 0 €.

Evidencia: readme-plugins.txt · SHA-256 4e4c4b15…c016c3

MEDIO	3.6 Enumeración de usuarios vía author-sitemap

Qué se observó. El author-sitemap.xml (Yoast) lista los autores: cliente-ejemplo (act. oct 2022) y agencia-externa-0 (act. ene 2025).

Por qué importa. Los nombres de autor suelen ser los nombres de usuario, mitad de las credenciales de acceso. Facilita fuerza bruta, sobre todo con plugins desactualizados y sin cabeceras. (La gobernanza de la cuenta de agencia se trata en Capa 7.)

Qué hacer. Desactivar el sitemap de autores; plugin anti-enumeración (cubrir /?author=N y API REST); disociar slug del username. **Esfuerzo:** 15 min · 0 €.

Evidencia: author-sitemap.xml · SHA-256 e52b2d2e…1b92bb

Aspectos correctos verificados en Capa 3

• robots.txt correctamente configurado, con reglas WooCommerce y referencia al sitemap.
• sitemap.xml estructurado (Yoast), catálogo de productos actualizado 5 días antes del análisis (negocio activo).
• Servidor Apache sin versión expuesta.

Capa 4 — Credenciales filtradas

POSITIVO **4.1 Sin emails corporativos expuestos en la web**

El HTML de la web y de la página de contacto no revela direcciones de correo en texto plano ni ofuscadas; el contacto se canaliza por formularios (Contact Form 7). Reduce spam, phishing dirigido y scraping. Buena práctica, frecuentemente incumplida por pymes.

INFORMATIVO **4.2 Verificación de filtraciones requiere colaboración**

Qué se observó. Consulta a Have I Been Pwned (Pwned Websites) sin localizar los dominios del cliente. La verificación por cuenta requiere conocer las direcciones concretas, que no son públicas.

Recomendación al cliente. Identificar emails corporativos activos y consultarlos en haveibeenpwned.com; para los expuestos: cambiar contraseña, revisar reutilización, activar 2FA; activar el aviso gratuito "Notify me".

Capa 5 — Suplantación y marca

POSITIVO **5.1 Registro defensivo de typosquatting**

Qué se observó. dnstwist identificó una sola variante registrada: ejemplo-clientte.es (omisión de una "s"), bajo control del cliente o su agencia (mismo correo, mismo DNS, IPs del mismo rango, redirige al principal).

Recomendaciones. Verificar titularidad a nombre del cliente; ampliar a variantes semánticas (al menos producto-estrella.es); monitorizar Certificate Transparency (Cert Spotter, gratuito); verificar marca en OEPM (la DOP protege el producto, no necesariamente el nombre comercial).

Evidencia: dnstwist-cliente.csv (f7f79c01…0b18) · whois-typosquat.txt (a2513797…de669d)

MEDIO **5.2 Typosquat defensivo sin HTTPS; redirección subóptima**

Qué se observó. ejemplo-clientte.es redirige al principal solo por HTTP; por HTTPS falla por ausencia de certificado. Además encadena cuatro saltos hasta el destino.

Por qué importa. Los navegadores modernos fuerzan HTTPS y la mensajería previsualiza por HTTPS; en esos casos la protección no funciona y el usuario ve una advertencia. La cadena de cuatro saltos añade latencia y penalización SEO. La configuración sugiere una regla antigua nunca actualizada tras la migración a HTTPS.

Descubrimiento colateral. Plugin Really Simple Security identificado vía cabecera X-Redirect-By.

Qué hacer. Emitir certificado para el defensivo (Let's Encrypt gratis); reducir a un único salto hacia https://www.ejemplo-cliente.es/; aplicar lo mismo al .com. **Esfuerzo:** 1 h · 0 €.

Evidencia: redirect-typosquat.txt (e3b0c442…b855, fichero vacío que documenta el fallo SSL) · redirect-http-typosquat.txt (cc811743…e8b3d)

ALTO **5.3 Servicio Nextcloud expuesto en subdominio no inventariado**

Qué se observó. Los logs Certificate Transparency revelaron archivo.ejemplo-cliente.es, no detectable por DNS estándar al dominio raíz. Aloja una instancia de Nextcloud (almacenamiento/colaboración) sobre PHP 8.2.31 y Plesk, con login propio. Su configuración de seguridad es **excelente** (CSP con nonces, X-Frame-Options, cookies Secure+HttpOnly+SameSite, noindex), en contraste con la web principal.

Por qué importa. El nombre (archivo.) y el software sugieren un repositorio documental interno, potencialmente con información sensible, expuesto a internet y posiblemente fuera del radar de mantenimiento.

Limitación. No se realizó análisis de vulnerabilidades por carecer de autorización; solo constatación e identificación pasiva.

Recomendaciones. Confirmar inventario y responsable; auditoría específica con autorización (versión, 2FA, cifrado en reposo, enlaces compartidos, logs); considerar restricción por IP/VPN; replicar sus cabeceras en la web.

Evidencia: archivo-subdomain-check.txt · SHA-256 b8d80db0…92c43b

Aspecto correcto verificado en Capa 5

• Sin suplantadores externos: las consultas a Certificate Transparency para variantes con "cliente-ejemplo" y "producto-estrella" no devolvieron dominios de terceros con certificado (verificado tras prueba de control del servicio).

Evidencia: subdominios-cliente.txt · SHA-256 148ccc55…97094b

Capa 6 — Analítica y trazabilidad

CRÍTICO **6.1 Google Analytics roto: medición inactiva**

Qué se observó. El HTML mezcla dos generaciones incompatibles de Google Analytics: sintaxis y librería antiguas (_gaq, ga.js, descatalogadas desde 2014) con un identificador moderno GA4 (G-XXXXXXXXXX).

```
var _gaq = _gaq || []; _gaq.push(['_setAccount', 'G-XXXXXXXXXX']); _gaq.push(['_trackPageview']); ga.src = '...google-analytics.com/ga.js';
```

Por qué importa. ga.js ya no es servida por Google y no es compatible con identificadores GA4. **El código no envía datos a ninguna parte.** El cliente probablemente cree que mide, pero recibe cero datos desde 2023. Toda decisión basada en analítica (tráfico, fuentes, conversiones, ROI, embudo, abandono de carrito) se toma sin datos. Se amplifica por ser una tienda online.

Qué hacer. Verificar el panel GA4 (probablemente vacío); sustituir por la implementación gtag.js correcta; considerar Google Tag Manager dado WooCommerce; verificar en Real-Time. Alternativa: plugin Site Kit by Google. **Esfuerzo:** 30-60 min · 0 €.

Evidencia: web-medicion.html líneas 1612-1618 (d3a9c569…1b49b1) · hallazgo-medicion.txt (d9cac63c…3a7be)

CRÍTICO **6.2 Tracker Mailchimp cargado antes del consentimiento**

Qué se observó. La web carga el "Mailchimp WooCommerce Pixel Tracking" mediante scripts incluidos directamente en el HTML, ejecutados **antes** de mostrar el banner de cookies e independientemente de lo que el usuario decida. El banner, por lo demás, está bien diseñado (Configurar/Aceptar/Rechazar con igual accesibilidad, panel granular), pero es **cosmético**: informa, no bloquea.

Por qué importa. Posible infracción del art. 22.2 LSSI (consentimiento previo) y del art. 6 RGPD (base legal). Transferencia internacional a Mailchimp (Intuit Inc., EE.UU.) que requiere base legal aplicada antes de la transferencia. Sanciones AEPD análogas a pymes: típicamente 1.500-5.000 €, hasta 30.000 € en casos graves.

Qué hacer. Configurar bloqueo previo de scripts no esenciales (o sustituir por Complianz / Borlabs / Cookie Notice); documentar base legal de la transferencia (DPA, Data Privacy Framework); actualizar la Política de Privacidad; extender el bloqueo a Stripe, YouTube e Instagram. **Esfuerzo:** 2-5 h · 0-300 €.

Evidencia: web-medicion.html líneas 3879/3881 y 3643+ · SHA-256 d3a9c569…1b49b1

Aspectos verificados en Capa 6

• Banner de cookies bien estructurado (el problema es funcional, no de diseño).
• Sin trackers de Meta/Facebook.
• Cookies de Stripe presentes por la pasarela; deben incluirse en el bloqueo previo.

Capa 7 — Continuidad y propiedad

POSITIVO **7.1 Infraestructura de correo con filtrado externo profesional**

Infraestructura de correo segmentada: servidor y SMTP en proveedor de hosting, webmail externalizado (CNAME a servicio-correo-proveedor.es), y MX/POP apuntando a un rango de operador de tránsito (Países Bajos, INFRA-AW), consistente con filtrado anti-spam intermedio. Capa profesional en frontera que mejora la entregabilidad. *Observación menor:* ftp.ejemplo-cliente.es resuelve a la web, no a un FTP real (alias legacy, recomendable eliminar sin urgencia).

Evidencia: subdominios-comunes-dns.txt (7371a4b7…39f712) · whois-ip-correo.txt (4a62a96b…93f67)

POSITIVO **7.2 Dominios paralelos consolidados en infraestructura única**

ejemplo-cliente.com comparte con el principal los mismos servidores DNS (dns-proveedor.com) y la misma IP (X.X.X.X), confirmando control por el mismo titular. *Matiz:* la consolidación en un único proveedor facilita la gestión pero elimina la redundancia ante un incidente del proveedor. Observación menor.

Evidencia: dig-com-ns.txt (fc66d4c3…b4a7b1e731) · dig-com-a.txt (2211ad74…0902fcd)

MEDIO — 7.3 Nextcloud autogestionado con propiedad incierta

Qué se observó. archivo.ejemplo-cliente.es usa infraestructura diferenciada: certificado Let's Encrypt (vs CA comercial de la web), Plesk + PHP 8.2 (vs Apache/WordPress), cabeceras estrictas (vs mínimas). Certificado emitido 08/04/2026, validez 90 días con renovación automática esperada.

Por qué importa. La discordancia sugiere gestión independiente, posiblemente por entidad distinta de quien mantiene WordPress. ¿Quién es el responsable? ¿Está el cliente al corriente? ¿Quién renovará la licencia de Plesk (de pago) si esa persona desaparece?

Recomendaciones. Documentar propiedad y administración; verificar titularidad de la licencia de Plesk y migrarla al cliente si procede; inventariar el sistema; considerar unificar la gestión técnica.

Evidencia: cert-archivo.txt · SHA-256 65bed2e6…961a107

ALTO — 7.4 Cuenta de proveedor externo con acceso reciente

Qué se observó. La cuenta agencia-externa-0 (agencia Agencia Externa) tiene última actividad (ene 2025) posterior a la del autor principal del negocio (oct 2022).

Por qué importa. Sugiere que un proveedor externo dispone de cuenta con privilegios y ha estado más activo que el propio cliente. Es habitual olvidar revocar accesos cuando una relación termina. Riesgo de gobernanza.

Recomendaciones. Revisar todas las cuentas con privilegios; confirmar contrato de mantenimiento vigente y accesos que justifica; revocar/degradar cuentas sin justificación; revisión semestral; activar 2FA en cuentas administrativas.

Evidencia: author-sitemap.xml · SHA-256 e52b2d2e…1b92bb

4. Correlaciones entre capas

Conecta hallazgos que, por separado, parecen menores, pero juntos elevan el riesgo o explican el estado del cliente. Es el valor diferencial de una revisión que mira el conjunto.

Correlación A — Quién hizo el trabajo, y por qué quedó a medias

Implicados: 1.x, 3.3, 3.5, 5.3, 3.6+7.4. Conviven configuraciones de alta calidad (SPF -all, TLS A+, cabeceras impecables en el Nextcloud, bloqueo selectivo de plugins de riesgo) con olvidos llamativos (cabeceras ausentes en la web, DMARC a medias, analítica rota, Slider Revolution obsoleto). No es una pyme abandonada, sino una que recibió trabajo competente sin mantenimiento continuo coordinado. La cuenta de agencia activa y el Nextcloud autogestionado aparte sugieren varias manos técnicas sin coordinación central.

Implicación. El cliente no necesita rehacer nada; necesita visión unificada y mantenimiento periódico. Ese es el servicio que justifica esta auditoría.

Correlación B — Riesgo de suplantación de marca

Implicados: 2.1, 2.2, 5.1/5.2. El correo puede suplantarse (DMARC no protege ni reporta), no hay forma de detectar campañas (sin rua), y la protección de dominios confundibles es parcial (sin HTTPS). Para una marca con DOP, escenario favorable a suplantación dirigida a clientes y distribuidores. **Acción coordinada:** cerrar DMARC, confirmar DKIM y completar HTTPS de los defensivos; las tres se refuerzan entre sí.

Correlación C — Tienda online que ni mide ni cumple

Implicados: 6.1, 6.2, 3.1, 3.4. La tienda está en la peor combinación: no mide lo que sí podría medir legalmente (GA4 inactivo) y mide lo que no debería sin consentimiento (Mailchimp libre). La ausencia de CSP y los plugins desactualizados elevan el riesgo de robo de datos en pago (Magecart). Atendidos juntos, transforman la tienda de "riesgo legal + ceguera analítica" a "medición correcta + cumplimiento + protección de pagos". Es la intervención de mayor retorno.

5. Plan de remediación priorizado

#	Hallazgo	Crit.	Plazo	Esfuerzo	Coste
1	6.1 Reparar Google Analytics	Crítico	<7 d	1 h	0 €
2	6.2 Bloqueo previo de cookies	Crítico	<7 d	1-2 h	0-300 €
3	3.4 Actualizar Slider Revolution y tema	Alto	<30 d	2-4 h	~25-85 USD
4	5.3/7.3 Inventariar y asegurar Nextcloud	Alto	<30 d	2-3 h	variable
5	7.4 Revisar cuentas con acceso	Alto	<30 d	1-2 h	0 €
6	3.1 Configurar cabeceras de seguridad	Alto	<30 d	1-2 h	0 €
7	2.1 Completar y escalar DMARC	Alto	30-60 d	1 h+	0 €
8	1.1 Renovar dominios (5 años)	Alto	<30 d	1 h	~30 €
9	2.2 Confirmar/activar DKIM	Medio	<90 d	30 min	0 €
10	5.2 Cobertura HTTPS de defensivos	Medio	<90 d	1 h	0 €
11	3.5 Bloqueo universal de readme	Medio	<90 d	15 min	0 €
12	3.6 Desactivar enumeración de usuarios	Medio	<90 d	15 min	0 €
13	1.2 Activar DNSSEC	Medio	<90 d	30 min	0 €
14	Menores (ftp legacy, OCSP, CBC)	Bajo	—	—	0 €

Coste económico total estimado: entre 60 € y 450 €, más horas técnicas. La mayor parte de los hallazgos críticos y altos se resuelven sin coste de licencias, solo con tiempo técnico.

6. Lo que NO se ha encontrado

Verificado y **no** encontrado (información tan relevante como los hallazgos):

- Certificado TLS válido, cifrado A+ sin vulnerabilidades conocidas.
- Sin emails corporativos expuestos a scrapers.
- Sin dominios del cliente en brechas públicas conocidas.
- Sin dominios suplantadores externos con certificado emitido.
- Sin subdominios huérfanos ni proliferación de entornos olvidados.
- Sin protocolos de cifrado obsoletos habilitados.
- Sin trackers de Meta/Facebook.
- Infraestructura de correo con filtrado anti-spam profesional.
- Bloqueo de transferencia de dominio (anti-secuestro) activado.

Estos puntos pueden cambiar. Se recomienda repetir la revisión cada 6-12 meses o tras cualquier cambio significativo (migración, cambio de agencia, incidente).

7. Anexo — Cadena de custodia ligera de evidencias

Todas las evidencias se conservan con su hash SHA-256 durante 90 días desde la fecha de este informe. La integridad de cada fichero puede verificarse recalculando su hash.

Nota de la versión anonimizada: los nombres de fichero y valores hash de esta tabla son ilustrativos y se conservan únicamente para mostrar la estructura de la cadena de custodia. No corresponden a ficheros descargables en esta versión pública.

Archivo	Capa	SHA-256
whois-cliente.txt	1	`9724cf912902d1eace47ceebcdbf05b91f2efd0339d0af9721bc19b267dae4c5`
dig-cliente.txt	1	`543cc3fb994d8e678a0567a725628f9ebb56ff2572287c938b6fca0b989171f2`
dmarc-cliente.txt	2	`a6fb3826df04cbf64f428c3b1373dc0b9f22b51e4270f945bac440858331510a`
dkim-cliente.txt	2	`b2bd538423265f5e596920a102baa347ab94eb5912f07025d85a0a49ba243b71`
headers-cliente-es.txt	3	`79df303aa6b047344f4eeaeb555fae79ba5a429fec864e79f487a957f86f63b3`
tls-cliente.txt	3	`4f08c1ac59651d09de5abeec1d18775b0b6503bf1e941dc1edd6da6d0b151b4f`
testssl-cliente.txt	3	`8b031538064e7d7504f68c130396e27b1e201de5b2050b9ed838309d86ed72a1`
web-cliente.html	3	`82b233b38add38e046bc3c53afd16a597c70b2628bd941e3e8494184f1375ea3`
hallazgo-generator.txt	3	`2d11daf3a0882c097e69d01e39baa307c95093da51e49cb512d8c458abf3273d`
hallazgo-plugins.txt	3	`b85cff650da6f4150eb5cf5030d931f34d1c103de1b4147ce550af5432c67374`
readme-plugins.txt	3	`4e4c4b15262561f0a2bdfbda92e72a98992d57a3a1767815bd2a5bab55c016c3`
robots-cliente.txt	3	`c356d3b91491bc659c2740586fcd7df58b5088fee61db6495513f5a77a65bc8a`
sitemap-cliente.xml	3	`c3d5974637a8094b90decaebffcb3a2ec6956b03ab851ee68dc13efe43477c07`
author-sitemap.xml	3	`e52b2d2e228afcc44aeabedbfe632f485f07f9ea330497def338a99fa61b92bb`
dnstwist-cliente.csv	5	`f7f79c0112ce7c6cf8ce7e99351cf51eee6d6f1ea58610a5d62d948d05670b18`
whois-typosquat.txt	5	`a25137979a57166287901e0667861d3004de00c5a698285497bf590001de669d`
redirect-typosquat.txt	5	`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`
redirect-http-typosquat.txt	5	`cc8117436ddd4538c4cc67ea0e6d08c2d4cd5a1f75be7c2bc2962c0c2a7e8b3d`
archivo-subdomain-check.txt	5	`b8d80db0aa520a7d0dc5ddbdc0014a271c8476c65488bd020dd10e2d9d92c43b`
subdominios-cliente.txt	5	`148ccc554cb043d169d2e92b9470d97d7be15dd16794fc13a66dcecd6b97094b`
web-medicion.html	6	`d3a9c569ddebe2fae8bb1a89688b5fd6122f3358e7783bdabbd5a6940d1b49b1`
hallazgo-medicion.txt	6	`d9cac63c40f6878fa0d1d26e4ef922e97bb11d5e9614a358ba664dc88d53a7be`
subdominios-comunes-dns.txt	7	`7371a4b79f2116329ff470b06d818bcc482d49dac57b0d13dacf00309b39f712`
whois-ip-correo.txt	7	`4a62a96bf3812d8dcdd81a89f17011b757d2162d78f2525eb7e586020ff93f67`
dig-com-ns.txt	7	`fc66d4c3f4756d5e4a0a8f20b1941c83c229c977fe3b4aa996813e44b7a1e731`
dig-com-a.txt	7	`2211ad74611c99d3f5933c38fb835c33fb8c59acf44a7a07fcd04e1170902fcd`
cert-archivo.txt	7	`65bed2e6bae3fca4320de6c99b1fdf4eeea2bf5811c985986e6a18149961a107`

8. Anexo Técnico A — Regla de bloqueo de archivos informativos

Regla para .htaccess (Apache) que bloquea el acceso público a readme/changelog/license de plugins y temas (Hallazgo 3.5). **Requiere backup previo del .htaccess y prueba en entorno controlado.**

```
# Bloqueo de archivos informativos de plugins y themes <IfModule mod_rewrite.c> RewriteEngine On
RewriteRule
^wp-content/(plugins|themes)/.+/(readme|changelog|license|README|CHANGELOG|LICENSE)\.(txt|md|html?)$ -
[F,L,NC] </IfModule> <FilesMatch "(?i)^(readme|changelog|license)\.(txt|md|html?)$"> Require all denied
</FilesMatch>
```

Alternativa: usar un plugin de hardening (Wordfence, iThemes Security) que implementa esta protección automáticamente, sin editar ficheros del servidor.

9. Declaración del autor

El presente informe ha sido elaborado siguiendo una metodología documentada y reproducible, sobre información de acceso público, sin acceso a sistemas internos del cliente. Las conclusiones se basan exclusivamente en la evidencia recogida durante la ventana de análisis indicada (16-20 de mayo de 2026) y reflejan el estado observable en ese momento. No se han manipulado, omitido ni interpretado de manera sesgada los hallazgos. Donde una herramienta presentó limitaciones, se documenta explícitamente.

El autor declara no tener conflicto de interés con el cliente ni con terceros mencionados en este informe.

Dragos C.I. Andrei
Málaga, a 20 de mayo de 2026

Fin del informe · Referencia AED-EJEMPLO-001