DOCUMENTO TÉCNICO · MARCO PROPUESTO · VERSIÓN 1.0

De la detección a la mitigación

Una arquitectura medible para responder al DNS Abuse: procedencia de las pruebas, medidas proporcionadas, rendición de cuentas pública y recurso rápido, concebida para someterse a prueba y no para limitarse a formular afirmaciones.

- Publicado el 2 de agosto de 2026
- PhishDestroy Investigación
- Borrador para consulta pública
- No ha sido revisado por pares

PD-WP-2026-01 · Version 1.0 · 2026-08-02
https://phishdestroy.io/es/dns-abuse-enforcement-framework

RESUMEN

PROPUESTA INDEPENDIENTE · NO ES UN PROGRAMA DE ICANN

Conclusión directa. El ecosistema contractual de «gTLD» presenta una brecha cuantificable entre el uso malicioso de un dominio, validado técnicamente, y la mitigación efectiva. Los estudios publicados muestran que muchas campañas de phishing operan durante horas o días, mientras que los procedimientos de cumplimiento contractual pueden desarrollarse a lo largo de varios días laborables. El modelo de escenario descrito muestra cómo el retraso aumenta los beneficios esperados de la campaña; el rango del 60 al 85 % es la estimación central y comprobable del artículo sobre el perjuicio posterior a la notificación, no una estadística establecida para todo el fraude mundial. La estimación de ingeniería de entre 100 y 150 dólares se refiere a la recopilación y el procesamiento inicial de un corpus definido de datos de zona, de Transparencia de Certificados y de fuentes públicas, no al coste total de la revisión jurídica o la ejecución. El artículo propone pruebas firmadas, objetivos de respuesta cuantificables, la escalación automática de los casos validados, medidas correctivas proporcionadas, rendición de cuentas pública y un procedimiento de recurso rápido. No propone otorgar a los denunciantes acceso directo a los controles de suspensión de dominios.

FUENTE PRIMARIA
Respaldado directamente por un documento oficial o un estudio publicado.

MODELO ILUSTRATIVO
Un cálculo reproducible cuyos datos de entrada son hipótesis, y no medias de mercado.

PROPUESTA DE POLÍTICA
Un diseño presentado para su consulta, prueba y revisión.

01 Pregunta de investigación, alcance y nivel de prueba

La pregunta es más concreta que «¿quién falló?»: **¿qué retrasos observables entre las pruebas validadas y una actuación proporcionada son evitables, y qué intervención reduce el perjuicio a las víctimas sin generar falsos positivos o daños colaterales inaceptables?**

El ámbito de aplicación es el ecosistema de gTLD contemplado en el contrato: titulares de dominios, revendedores, registradores, registros y la función de cumplimiento contractual de ICANN. Los

proveedores de alojamiento web, las redes de distribución de contenidos (CDN), los navegadores, los servicios de pago, las plataformas publicitarias, los CERT nacionales y las fuerzas del orden solo se incluyen en la medida en que afecten a la cadena de pruebas o de respuesta. Los TLD de código de país tienen una gobernanza diferente y no se considera que estén sujetos a los contratos de gTLD de ICANN.

Estado de las tesis principales

- El artículo analiza ICANN como una institución de gobernanza privada y de cumplimiento contractual dentro del ecosistema de la «gTLD». ICANN no es un organismo regulador gubernamental ni una autoridad encargada de hacer cumplir la ley, pero acredita a los registradores, celebra contratos con los operadores de registros y vela por el cumplimiento de dichos acuerdos; ese ámbito de competencia limitado no exime a la institución de su responsabilidad.
- El intervalo del 60 al 85 % es una estimación cuantitativa fundamental en el modelo de daños del artículo. Se presenta como una estimación comprobable derivada de supuestos explícitos y observaciones de casos concretos, y no como una estadística ya establecida para el fraude a nivel mundial. El siguiente paso para aportar pruebas consiste en publicar un conjunto de datos a nivel de incidente que alinee las marcas de tiempo de detección, notificación, mitigación y daño.
- La cifra de entre 100 y 150 dólares es una estimación presupuestaria de ingeniería comprobable para la recopilación continua y la clasificación inicial de un conjunto definido de datos de zonas accesibles, de «Certificate Transparency» y de fuentes públicas sobre infraestructura básica. No se trata del coste de la visibilidad global completa, la revisión jurídica, los recursos, la alta disponibilidad ni la aplicación de la normativa. Por lo tanto, el documento lo trata como un punto de referencia que puede reproducirse con una carga de trabajo publicada, un inventario de fuentes y un registro de costes, y no como un precio universal ya demostrado. Esa distinción matiza la afirmación sin eliminar la asimetría de costes que se está analizando.
- La comparación de tres semanas que se presenta en el artículo se refiere a la latencia en el cumplimiento, no a un acuerdo de nivel de servicio (SLA) universal para el cierre de dominios. El artículo de «ICANN»... Preguntas frecuentes sobre el cumplimiento contractual establece que la mayoría de los tipos de reclamaciones pueden pasar por tres períodos sucesivos de respuesta de cinco días laborables antes de que se proceda a una escalación formal, mientras que muchas campañas maliciosas permanecen activas durante horas o días. Los contratos exigen, por separado, la adopción de medidas de mitigación rápidas y adecuadas tras la obtención de pruebas que justifiquen la intervención. [2] [4]
- En el caso de un registro malicioso verificado y con un único propósito, `serverHold` Es una de las medidas correctivas más disruptivas a nivel de «DNS», ya que elimina la delegación de la zona. No es una solución universal: también puede afectar al correo electrónico, a los subdominios y a los servicios legítimos; las respuestas almacenadas en caché pueden permanecer hasta que caduque el TTL; y los servicios comprometidos o compartidos pueden requerir medidas de mitigación más específicas. [4] [7]

CONTRIBUCIÓN A LA INVESTIGACIÓN

La propuesta es falsable. Un estudio piloto puede comparar cohortes de tratamiento y control en tiempo hasta el triaje, tiempo hasta la mitigación, indicadores de pérdida para las víctimas, recurrencia, falsos positivos, tiempo de reversión e impacto colateral.

02 Lo que demuestran las fuentes primarias

$165.1M

Financiación operativa de ICANN para el ejercicio fiscal 2027

Presupuesto aprobado para el ejercicio fiscal 2027. Escala contextual; no representa el gasto destinado al DNS Abuse. [1]

191,561

Denuncias por phishing y suplantación de identidad en el IC3 en 2025

Categoría de denuncias al IC3 con mayor número de casos; 215,8 millones de dólares en pérdidas atribuidas directamente. [10]

24 h

Mediana de vida útil en un estudio de 2021

Resultado específico de un conjunto de 1.288 dominios de phishing; no es una duración universal. [11]

Sin SLA fijo

Plazo universal de desactivación

Las modificaciones de 2024 exigen una mitigación «rápida» y «adecuada», no un único plazo mundial. [2] [3]

PROPUESTA	ESTADO	LO QUE SE PUEDE AFIRMAR
El phishing es DNS Abuse	VERIFICADO	El phishing es expresamente una de las cinco categorías cubiertas por las modificaciones contractuales de 2024 aplicables a los gTLD. [2]
Los registradores deben actuar	VERIFICADO	Los registradores deben actuar con prontitud cuando dispongan de pruebas accionables de que un nombre patrocinado se utiliza para DNS Abuse. [2]
Los operadores de registro deben actuar	VERIFICADO	Los operadores de registro deben actuar con prontitud cuando determinen razonablemente, a partir de pruebas accionables, que un nombre registrado se utiliza para DNS Abuse; la medida adecuada sigue dependiendo del contexto. [3]
`serverHold` elimina la delegación	VERIFICADO	Se trata de un estado EPP establecido por el servidor. Las respuestas almacenadas en caché de DNS pueden permanecer hasta su caducidad, y la acción afecta a todo el dominio registrado. [7]
Todo DNS Abuse puede observarse en CZDS o CT	FALSO	CZDS y Certificate Transparency son sensores valiosos, pero no ofrecen una visión completa ni en tiempo real de todo uso de dominios. [8] [9]

El primer informe semestral de ICANN sobre la aplicación de las modificaciones de 2024 registró 192 investigaciones, más de 2.700 dominios suspendidos, más de 350 páginas de phishing desactivadas y dos notificaciones formales de incumplimiento (Notices of Breach). Estas cifras no prueban que los

controles actuales sean suficientes, pero sí descartan la afirmación absoluta de que el sistema no actúa. [5]

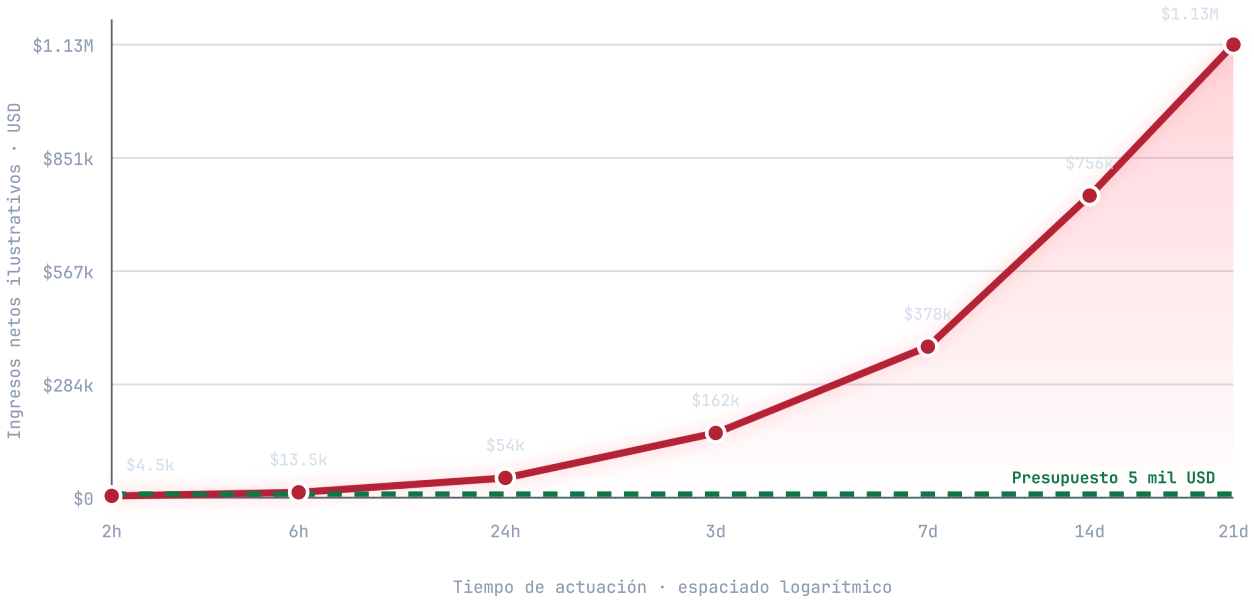
03 Por qué la latencia de respuesta sigue siendo un objetivo de investigación legítimo

Algunas campañas de phishing operan en un plazo de horas o días. Bijmans et al. indicaron, en un estudio de 2021, una vida útil media observada de 45 horas y una mediana de 24 horas para 1.288 dominios de phishing. Un estudio de 2026 sobre dominios de phishing recién registrados reveló una distribución muy asimétrica: para 14 112 dominios con una vida útil cuantificable, la media fue de 8,6 días y la mediana, de un día. Ninguna de las dos muestras puede generalizarse a todas las clases de amenazas, pero ambas muestran por qué un proceso que se mide únicamente en días laborables puede pasar por alto campañas de corta duración. [11] [12]

> **EL DESFASE TEMPORAL MEDIDO**
>
> Estos estudios no determinan la proporción del perjuicio financiero que se produce tras la notificación, pero sí ponen de manifiesto un desajuste temporal: un proceso cuyas primeras fases de cumplimiento informal pueden prolongarse hasta quince días hábiles no puede, por sí solo, servir como respuesta a incidentes en campañas cuya duración media ronda el día. Por lo tanto, el plazo de 21 días que se menciona a continuación corresponde a un escenario de latencia en el cumplimiento, y no es una etiqueta para un «SLA de ICANN» universal.

FIGURA 1 · RESULTADO ACUMULATIVO ILUSTRATIVO DE LA CAMPAÑA

MODELO · ESPACIADO TEMPORAL DE TIPO LOGARÍTMICO



La curva representa el escenario descrito en la sección 4; no se trata de datos de mercado observados. La disposición horizontal comprime los intervalos largos para facilitar la lectura. Fuente: modelo reproducible con datos de entrada publicados.

PRECAUCIÓN CAUSAL

Una vida útil más corta del dominio no implica automáticamente que se eviten pérdidas económicas. Los atacantes pueden cambiar de estrategia, utilizar sitios web comprometidos, modificar los canales de distribución o retirar el dinero antes de que se les detecte. El efecto causal debe medirse, y no deducirse únicamente a partir de la rapidez con la que se retira el contenido.

04 La economía de las operaciones fraudulentas como escenario reproducible

El activo económicamente relevante no suele ser la cuota de registro, sino el tráfico, los materiales creativos, la infraestructura y la confianza acumulados alrededor de un dominio. La intuición es plausible, pero su magnitud varía según la operación fraudulenta. Por ello, la calculadora expone todos los datos de entrada en vez de presentar un resultado hipotético como promedio observado.

DEFINICIÓN DEL MODELO

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Calculadora de escenarios

Modifica cualquier hipótesis. Los valores son meramente ilustrativos y no constituyen estimaciones del mercado típico del phishing.

MODELO ILUSTRATIVO

Presupuesto de la campaña (USD)

5000

Visitas diarias

2000

Tasa de conversión de víctimas (%)

1.5

Pérdida media por víctima (USD)

2400

Merma en la retirada de fondos (%)

25

Tiempo de actuación (horas)

24

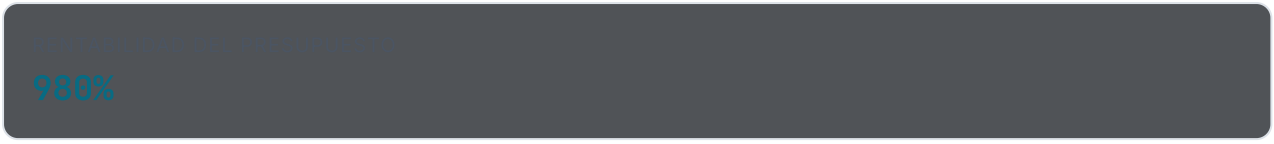
Visitas
2,000

Víctimas esperadas
30

Pérdidas brutas
$54,000

Pérdidas evitadas
$49,000

Tiempo de amortización
2.2 h



El número esperado de víctimas puede contener decimales porque el modelo expresa un valor esperado. Omite la disminución del tráfico, la retroalimentación de la detección, la migración, las víctimas repetidas y las distribuciones de incertidumbre.

▶ Ver la tabla de origen del modelo

05 Medir el daño evitable sin inventarse la precisión

La «pérdida tras la detección» solo puede constituir un resultado útil si la detección, la entrega y el perjuicio se definen de manera coherente. La marca de tiempo de una lista negra no es prueba de que el registrador haya recibido pruebas que permitan actuar. Una transacción de monedero no es automáticamente atribuible a un dominio concreto. El hecho de que un dominio deje de estar accesible no permite identificar qué actor ha provocado el cambio.

Esquema mínimo de eventos

EVENTO	MARCA DE TIEMPO OBLIGATORIA	PRUEBA MÍNIMA
Primera observación	`t_obs`	Sensor, hash de solicitud/respuesta, método de captura, fuente de reloj.
Validación técnica	`t_valid`	Indicador reproducible, identidad del revisor, categoría de amenaza y nivel de confianza.
Notificación entregada	`t_notice`	Acuse de entrega autenticado y versión del evidence envelope.
Acuse del actor responsable	`t_ack`	ID del caso y función de destino: host, registrador, registro, plataforma o autoridad.
Mitigación observada	`t_mitigate`	Estado de DNS, HTTP, pagos o plataforma, medido desde varios puntos de observación.
Recurso / restablecimiento	`t_restore`	Fundamento de la decisión, pruebas modificadas y verificación de la restauración.
Incidente con daños	`t_harm`	Informe de la víctima sin datos identificativos, transacción atribuible u otro indicador documentado.

INDICADOR DE RESULTADOS PROPUESTO

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

El numerador y el denominador deben seguir la misma regla de atribución. Los resultados deben indicar la cohorte, el intervalo de confianza, la censura a la derecha, las fuentes que faltan, el tratamiento de las víctimas duplicadas y la sensibilidad a la ventana de observación. La etiqueta «evitable» debe reservarse para un diseño causal o, como mínimo, para una comparación emparejada, y no para cualquier evento posterior a la notificación.

ESTIMACIÓN CENTRAL DEL MODELO · 60-85 %

El artículo mantiene un rango del 60 % al 85 % como estimación central de la proporción de daños atribuibles que se producen tras la detección y la notificación en la clase de incidentes objeto del modelo. Se trata de una estimación hipotética derivada de supuestos divulgados y observaciones de casos, no de una estadística medida para todos los fraudes a nivel mundial. Debería utilizarse para el análisis de sensibilidad hasta que un conjunto de datos a nivel de incidente concilie las observaciones, las pruebas validadas, la entrega, la mitigación y las marcas de tiempo del daño. La publicación de ese conjunto de datos constituye la prueba probatoria de la tesis, no una razón para descartarla.

06 El mapa institucional: la capacidad está distribuida

Ningún actor por sí solo ve ni controla el incidente en su totalidad. El registrador conoce la relación con el titular del registro; el registro controla el estado de los dominios que gestiona; el servidor y CDN controlan la distribución de contenidos; los navegadores y los proveedores de seguridad controlan las advertencias; los proveedores de pagos y monederos electrónicos pueden interrumpir las transferencias; y las autoridades pueden ordenar la conservación o la incautación. ICANN redacta y hace cumplir los contratos en el ecosistema gTLD, pero no gestiona un plano de control EPP universal.

01 · SEÑAL

Investigadores y sensores

Observan indicadores de contenido, infraestructura y víctimas; preservan la procedencia.

02 · SERVICIO

Host / CDN / plataforma

Puede retirar contenidos o bloquear el acceso con rapidez, a menudo sin modificar el dominio.

03 · PATROCINADOR

Registrador

Revisa el caso de abuso, contacta con el titular y puede establecer estados del lado del cliente.

04 · ZONA

Operador de registro

Controla el estado de EPP establecido en el registro y la delegación de la zona del TLD.

05 · CONTRATO

Cumplimiento Contractual de ICANN

Investiga el cumplimiento de las partes contratadas; no resuelve cada caso de fraude.

06 · DERECHO

CERT / autoridades

Coordinan la respuesta y ejercen las facultades jurídicas propias de cada jurisdicción.

La capacidad distribuida no implica una responsabilidad disuelta. Un registrador patrocinador no se exime de sus obligaciones contractuales al delegar la gestión de los abusos a un revendedor; el registro controla el estado del EPP configurado en el servidor; ICANN vela por el cumplimiento de los términos contractuales. El registro de auditoría debe recoger no solo quién actuó, sino también quién recibió pruebas procesables, quién redirigió el caso, quién no respondió o quién incumplió una obligación asignada. La autoridad legal recae en el agente facultado para aplicar una medida; la rendición de cuentas también abarca los incumplimientos documentados.

Concentración de la financiación y una hipótesis comprobable sobre el conflicto de incentivos

$165.1M

Financiación para las operaciones de «ICANN» del ejercicio fiscal 27

Se ha aprobado el presupuesto del caso base para el ejercicio fiscal 27. [1]

≈98.1%

fuentes de ingresos por registro y por servicios de registro

Aproximadamente 162,0 millones de dólares del plan de financiación de 165,1 millones de dólares. [1]

70.7%

solo las comisiones por transacción

$116.8M tied to billable domain transactions. [1]

Por lo tanto, la estructura de financiación se concentra en gran medida en los pagos de las partes contratantes cuyos acuerdos hace cumplir ICANN, y una gran parte de ella varía en función de las transacciones de registro facturables. Esto establece una dependencia estructural y plantea una cuestión legítima de conflicto de incentivos. Esto hace que *no*, por sí solo, no demuestra una falta de aplicación intencionada de la normativa ni una «captura regulatoria» consumada. La hipótesis de la captura debería contrastarse con los tiempos de respuesta en cada caso concreto, los resultados de la aplicación de la normativa, las sanciones, la reincidencia en los abusos y el papel de las partes interesadas financiadas en las decisiones sobre políticas y su aplicación.

07 La base contractual para 2024 — y lo que no especifica

Las modificaciones globales de abril de 2024 del Registrar Accreditation Agreement y del Base Registry Agreement establecieron obligaciones expresas para mitigar el DNS Abuse. Los registradores deben actuar con prontitud cuando dispongan de pruebas accionables de que un nombre patrocinado se utiliza para DNS Abuse. Los operadores de registro deben actuar con prontitud cuando determinen razonablemente, a partir de pruebas accionables, que un nombre registrado se utiliza para DNS Abuse. En ambos casos, la medida adecuada depende del contexto, la gravedad y el impacto colateral. [2] [3]

Tres líneas temporales que a menudo se confunden

CRONOLOGÍA	A QUÉ SE APLICA	LO QUE NO SIGNIFICA
24 horas	Revisión, conforme a la sección 3.18.3 del RAA, de informes bien fundamentados sobre actividades ilegales («Illegal Activity») enviados al contacto específico por autoridades policiales, de protección del consumidor, cuasigubernamentales u otras similares.	No se trata de un plazo universal de suspensión de 24 horas.
«Con prontitud»	Adoptar una mitigación adecuada una vez alcanzado el umbral aplicable de pruebas accionables.	No equivale a un número fijo de horas ni exige la misma solución en todos los casos.
21 días	Puede constituir un plazo de subsanación tras una notificación formal de incumplimiento contractual.	No se trata de la duración habitual que se asigna a todos los dominios maliciosos detectados.

Esta flexibilidad tiene sus ventajas: un dominio universitario comprometido no debe tratarse como un dominio de phishing de uso único recién registrado. El problema en cuanto a la rendición de cuentas radica en que resulta difícil comparar lo que es «rápido» y lo que es «adecuado» sin marcas de tiempo publicadas, categorías de casos y códigos de resultado. La propuesta que figura a continuación incorpora medidas de evaluación y revisión sin pretender que un único plazo sirva para todos los casos.

08 El problema de los límites: se incluye el phishing; es posible que algunos tipos de estafa financiera no estén incluidos

El phishing está expresamente incluido en la definición contractual de DNS Abuse. La frontera más difícil comprende sitios que engañan con un nombre propio en vez de suplantar a un tercero identificable: determinadas plataformas de inversión falsas, tiendas fraudulentas, estafas de recuperación y esquemas para obtener firmas de monederos. Según los hechos, pueden tratarse

como abuso de contenidos web, fraude al consumidor u otra categoría jurídica, y no como DNS Abuse contractual.

> TÉRMINO DE INVESTIGACIÓN PROPUESTO
>
> **Verified Financial Harm Abuse (VFHA)**: uso documentado de un dominio para obtener fondos, credenciales de pago, claves privadas o frases semilla mediante engaño, con independencia de la suplantación de una marca. VFHA no forma parte de la terminología vigente de ICANN ni crea por sí solo una facultad contractual.

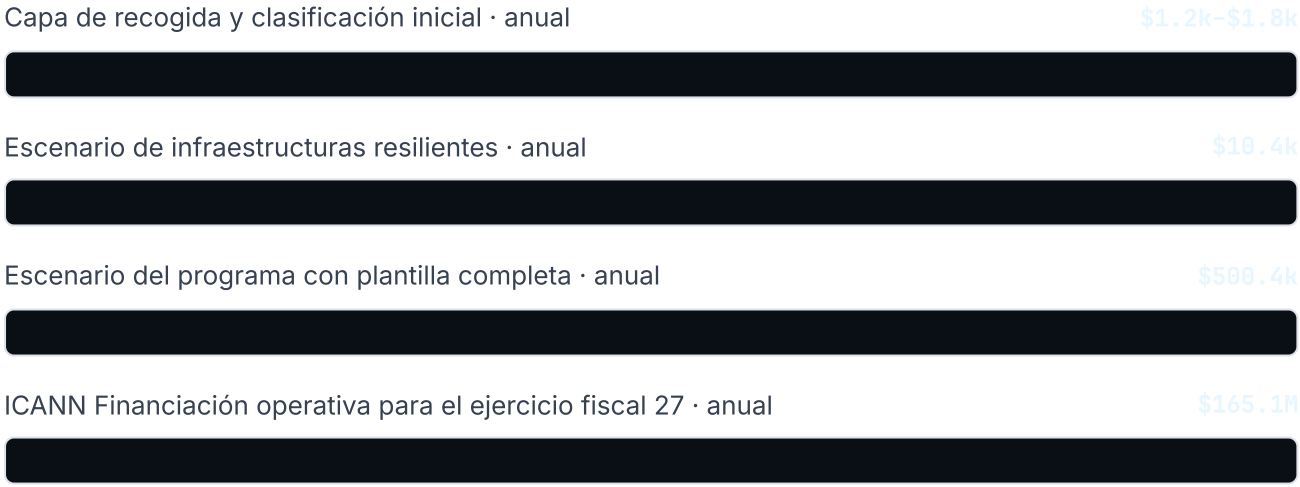
Una consulta de política pública podría examinar si una categoría estrecha y respaldada por pruebas como VFHA debe incorporarse a futuros contratos, a un marco de derivación intersectorial o al derecho nacional. Toda ampliación debería exigir una prueba precisa del daño, pruebas fiables, remedios proporcionados, revisión jurisdiccional y recurso. Las etiquetas vagas de «estafa» son insuficientes.

09 Lo que debe demostrar la afirmación sobre la supervisión de entre 100 y 150 dólares al mes… y lo que no puede demostrar

Un servidor estándar puede descargar instantáneas accesibles de los archivos de zona participantes de gTLD y calcular los cambios a nivel local, incorporar eventos seleccionados de Transparencia de Certificados y fuentes abiertas, normalizar cadenas de caracteres, calcular hash y priorizar candidatos. Se trata de un punto de referencia de ingeniería útil y comprobable, no de una «supervisión completa de Internet». En el segundo trimestre de 2026, Verisign informó de 401,6 millones de registros en todos los TLD; el CZDS abarca los archivos de zona participantes de gTLD en lugar de todos los TLD, y el CT registra certificados o precertificados registrados públicamente, en lugar de todos los dominios activos o maliciosos. [8] [9] [17]

CAPACIDAD	PROTOTIPO EN INFRAESTRUCTURA CONVENCIONAL	SERVICIO DE PRODUCCIÓN DE INTERÉS PÚBLICO
Ingesta de zonas/CT/feeds	Viable para un conjunto de fuentes definido	Recolectores redundantes, contratos con fuentes y supervisión de lagunas
Clasificación de cadenas y hash	Viable	Evaluación comparativa, detección de desviaciones, estudios sobre falsos negativos
Representación en el navegador	Subconjunto de muestra reducido	Flota aislada, puntos estratégicos regionales, contención de malware
Determinación jurídica	No incluida	Revisores cualificados y asignación de jurisdicción y facultades
Alta disponibilidad / conservación de pruebas	Normalmente ausente	Firmas respaldadas por HSM, registros de auditoría, copias de seguridad y respuesta ante incidentes
Recursos y restablecimiento	No incluido	Operaciones 24 horas al día, 7 días a la semana; escalado autónomo y objetivos de servicio

FIGURA 2 · CONTEXTO DE ORDEN DE MAGNITUD — ANCHURA LOGARÍTMICA · COSTES NO COMPARABLES



Los anchos logarítmicos permiten que los valores pequeños sigan siendo visibles. Las tres primeras cifras son hipótesis técnicas o de programa que requieren un punto de referencia publicado y no son presupuestos de proveedores. ICANN La financiación de las operaciones es una cifra verificada a escala institucional. Se trata de presupuestos deliberadamente no equivalentes: la comparación comprueba si la recogida y la clasificación básicas suponen un coste intrínsecamente prohibitivo, no si un programa completo de cumplimiento cuesta 100 dólares al mes.

10 Marco propuesto de respuesta a abusos verificados

El marco propuesto es una arquitectura de referencia, no un «interruptor de apagado» mundial automático. Normaliza el evidence envelope, el expediente de decisión y las marcas de tiempo, y

permite al operador autorizado elegir la medida eficaz con menor impacto colateral.

01 · INGESTA

Adquirir & preservar

Recopilar informes y observaciones; generar hashes de los artefactos en bruto; sincronizar los relojes.

02 · PROCEDENCIA

Normalizar las pruebas

Registrar el origen, el método, el historial de tratamiento y las dependencias de las fuentes.

03 · VALIDAR

Corroborar

Reproducir el comportamiento perjudicial y distinguir las pruebas independientes.

04 · EVALUAR

Riesgo & impacto colateral

Clasificar registros maliciosos, servicios comprometidos, alojamiento compartido y gravedad.

05 · RESPONDER

Notificar y mitigar

Asignar al responsable, el plazo previsto y la solución eficaz que menos trastornos cause.

06 · REVISAR

Auditoría & recurso

Publicar metadatos de resultados, medir el impacto y facilitar una reversión rápida.

Niveles de evidencia

E1 **Señal no verificada**

Una sola denuncia, coincidencia léxica o acusación basada en la reputación. Adecuado para la observación, pero nunca suficiente por sí solo para justificar una suspensión.

E2 **Comportamiento reproducido**

Captura con marca de tiempo que muestra el robo de credenciales, la distribución de malware o una ruta de transacción engañosa.

E3 **Corroboración independiente**

Al menos dos fuentes verdaderamente independientes o una prueba técnica reproducible, además de comprobaciones de la titularidad y el contexto.

E4 **Confirmación cualificada**

Autoridad, servicio afectado, titular de marca o pruebas validadas de víctimas, con una cadena de custodia respetuosa con la privacidad.

REGLA DE LA INDEPENDENCIA

Tres fuentes que copian la misma lista negra de origen constituyen una sola fuente, no tres. El gráfico de procedencia debe mostrar el origen compartido, la sincronización y la republicación por parte del proveedor.

11 Un evidence envelope mínimo y una API interoperable

El «API» debe crear un caso verificable y activar un temporizador de respuesta auditable; un informante no debe poder emitir directamente un comando de retención. Si un caso E3/E4 se refiere a un registro malicioso con un único propósito y caduca sin una decisión motivada o una mitigación efectiva, el sistema lo remite automáticamente al operador del registro o a otro agente con autoridad contractual o legal. A `serverHold` El comando solo puede proceder de un agente autorizado. La escalación automática y la autoridad del registro para actuar en caso de caducidad son cambios propuestos en la política, no afirmaciones sobre una autoridad ya existente. Cada transición de estado se firma y se añade al registro de auditoría.

POST /V1/CASES · EJEMPLO

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

Una respuesta satisfactoria devuelve el ID del caso, el actor receptor, el nivel de pruebas, los errores de integridad, el plazo previsto de revisión y una URL pública de transparencia. No debe prometerse un remedio concreto antes de que un actor competente evalúe su competencia y el impacto colateral.

12 Objetivos de respuesta propuestos, no plazos universales de desactivación

Los objetivos de nivel de servicio deben distinguir entre *acuse de recibo*, *triaje*, *decisión* y *mitigación eficaz*. Así puede medirse el rendimiento sin suponer que la suspensión sea siempre el resultado adecuado.

PERFIL DEL CASO	RECONOCER	OBJETIVO DE TRIAJE	OBJETIVO DE LA DECISIÓN	OPCIONES DE RESPUESTA HABITUALES
Robo E3/E4 de credenciales de pago o frases semilla mediante un registro malicioso de propósito único	15 min	1 h	4 h	Bloqueo de contenido; suspensión por el registrador o el operador de registro cuando esté autorizada; alertas en navegador y pagos.
Phishing de marca E3 o distribución de malware	30 min	2 h	6 h	Retirada por host/CDN, mitigación del dominio, sinkhole o aviso según el punto de control.
Dominio legítimo comprometido o inquilino de SaaS compartido	1 h	4 h	12 h	Aislamiento de rutas/cuentas y recuperación de la titularidad; evitar, en la medida de lo posible, la suspensión de los dominios registrados.
Fraude financiero con clasificación impugnada	4 h	12 h	24 h	Conservación, intervención en la plataforma o en el pago, remisión a la autoridad competente y resolución motivada.
Señal E1 o informe incompleto	Auto	24 h	Ninguna hasta su validación	Supervisar, ampliar y solicitar pruebas.

Son objetivos para el piloto. Los valores adecuados deben derivarse de la duración observada de las amenazas, la dotación, el coste de los errores y las restricciones jurídicas, y publicarse como distribuciones de cumplimiento, no como una única media.

13 Seguridad, garantías procesales, privacidad y modos de fallo

Una respuesta rápida sin las medidas de protección adecuadas puede convertir los datos erróneos en censura, sabotaje comercial o interrupciones en las infraestructuras. Por lo tanto, una arquitectura adecuada considera los falsos positivos y los daños colaterales como fallos de seguridad de primer orden.

MODO DE FALLO	CONTROL OBLIGATORIO	MEDIDA AUDITABLE
Denuncia maliciosa contra un competidor	Autenticación de los informantes, reputación de las fuentes, reproducción independiente y sanciones por abuso	Tasa de informes rechazados por informante; casos confirmados de manipulación
Circularidad de feeds presentada como consenso	Gráfico de procedencia y deduplicación de fuentes ascendentes	Recuento de fuentes independientes antes y después de corregir el linaje
Suspensión general de un dominio legítimo comprometido	Clasificación de la intención de registro y preferencia por mitigación a nivel de ruta	Porcentaje de dominios comprometidos; servicios legítimos afectados
Se han filtrado públicamente datos de las víctimas o detalles sobre los ataques	Divulgación por niveles, supresión de información, pruebas selladas y plazos de conservación	Incidentes relacionados con la privacidad; resultados de la revisión de la supresión de datos
Persiste una actuación indebida	Recepción de recursos 24/7, revisor independiente y proceso de restauración autenticado	Mediana y percentil 95 del tiempo de reversión
Una suspensión a nivel de registro interrumpe el correo o los subdominios	Inventario del impacto colateral, proporcionalidad del remedio y seguimiento posterior	Servicios interrumpidos por actuación; tasa de reversión

Salvaguardas procesales mínimas

1. Para cada medida restrictiva se registran el código de motivo, el nivel de evidencia y la persona responsable de la decisión.
2. El titular del registro puede obtener una exposición de motivos que respete la privacidad y presentar pruebas en contra.
3. Los recursos urgentes son revisados por una persona que no haya tomado la decisión original.
4. La reversión se propaga por el mismo canal firmado que la actuación original.
5. Las estadísticas agregadas sobre errores y restauraciones son públicas; el acceso a las pruebas confidenciales sigue estando restringido.

14 De una «puntuación de toxicidad» a un Índice de Calidad de la Respuesta que permite rendir cuentas

La puntuación pública de un registrador puede mejorar la rendición de cuentas, pero las clasificaciones simplistas se ven distorsionadas por el tamaño de la cartera, la cobertura de la fuente de datos, la composición de la clientela y el hecho de que los dominios se hayan registrado de forma maliciosa o se hayan visto comprometidos posteriormente. Una puntuación nunca debe justificar el bloqueo colectivo de todos los clientes de un registrador.

VECTOR DE CALIDAD PROPUESTO

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Si se requiere un índice compuesto para la gobernanza, las ponderaciones deben establecerse antes de la evaluación, someterse a pruebas de sensibilidad y a pruebas retrospectivas con casos no incluidos en el modelo. Los resultados deben estratificarse por TLD, tamaño del registrador, clase de amenaza y fuente de la evidencia. El resultado es una señal de responsabilidad, no un veredicto automatizado sobre el dominio.

15 Base de Datos Pública de Transparencia sobre DNS Abuse por niveles

Un registro de transparencia puede evitar disputas sobre si se envió una notificación, cuándo se entregó y qué medidas se tomaron a raíz de ella. Sin embargo, publicar todos los elementos podría poner en riesgo a las víctimas, los datos personales, los métodos de investigación y las vías de explotación activas. La solución es el acceso por niveles.

P

Registro público

ID del caso, indicador, categoría general, marcas de tiempo clave, nivel de prueba, funciones de los actores, código de resultado, estado del recurso y hashes de los artefactos sellados.

C

Vista de la parte contratante

Pruebas técnicas reproducibles, canal de contacto, contexto complementario e instrucciones de conservación.

R

Vista restringida para autoridades

Datos de víctimas, atribución financiera, material de investigaciones activas y cadena de custodia íntegra.

Cada actualización es de solo adición, lleva una marca de tiempo y está firmada. Las correcciones no borran el historial, sino que añaden un registro que sustituye al anterior. La búsqueda pública debe respetar las normas de conservación, impedir la identificación masiva de víctimas y ofrecer reparación en caso de datos personales inexactos.

16 Un piloto de seis meses con evaluación preregistrada

Un proyecto piloto útil debe ser lo suficientemente pequeño como para poder gestionarlo y lo suficientemente grande como para poner a prueba la cadena causal. Alcance sugerido: tres registradores voluntarios, dos operadores de registro, un socio de alojamiento/CDN, dos fuentes de investigación independientes y un comité de apelación cualificado. El protocolo del estudio y las definiciones de los resultados deben registrarse antes de asignar los casos.

MES 1

Protocolo y análisis jurídico

Definir las categorías, las autoridades, los niveles de evidencia, la evaluación del impacto en la privacidad y las condiciones de cese.

MES 2

Instrumentar el proceso existente

Medir las marcas de tiempo y resultados de referencia sin alterar el comportamiento de respuesta.

MES 3

Poner a prueba el evidence envelope

Introducir procedencia firmada, deduplicación y clasificación del impacto colateral.

MES 4

Probar objetivos de respuesta

Aleatorizar los casos elegibles o utilizar una implantación escalonada; supervisar los errores a diario.

MES 5

Ensayar recursos y fallos

Realizar simulacros de restauración, simulaciones de denuncias maliciosas realizadas por un red team y auditorías de los controles de acceso.

MES 6

Evaluación independiente

Publicar los tamaños del efecto, los intervalos de confianza, los datos que faltan, los efectos adversos, los costes y los materiales de replicación.

Resultados principales del estudio piloto

- Tiempo mediano y del percentil 90 desde la obtención de pruebas validadas hasta la aplicación de medidas de mitigación eficaces.
- Diferencia en el perjuicio atribuible tras la notificación o un indicador sustitutivo de la exposición de la víctima previamente especificado.
- Tasa de falsos positivos, gravedad de las actuaciones indebidas y mediana del tiempo de restablecimiento.
- Recurrencia en el mismo titular, clúster de infraestructura y campaña.
- Coste operativo directo por caso validado y por medida de mitigación efectiva.

REGLA DE DECISIÓN

Ampliar solo si el piloto demuestra una mitigación eficaz sustancialmente más rápida sin superar los límites preregistrados de falsos positivos, incidentes de privacidad, demora de recursos o interrupción colateral de servicios.

17 Conclusiones y recomendaciones verificables

La respuesta al DNS Abuse no es un filtro puramente técnico ni un problema que una institución pueda resolver por sí sola. Los contratos vigentes de 2024 establecieron obligaciones de mitigación sustantivas, pero dejan un margen considerable sobre las pruebas, los plazos y el remedio. Esa discrecionalidad es necesaria para la proporcionalidad; sin registros comparables, también dificulta evaluar el rendimiento.

1. **Normalizar el evidence envelope.** Adoptar campos comunes de procedencia, marca de tiempo y resultado para informantes, registradores, registros y proveedores de infraestructura.
2. **Medir las etapas por separado.** Publicar los tiempos de acuse, triaje, decisión, mitigación y recurso por clase de amenaza y nivel de evidencia.
3. **Distinguir entre un registro malicioso y una intrusión.** Es preferible aplicar medidas correctivas a nivel de ruta o cuenta en el caso de servicios legítimos que hayan sido comprometidos, y reservar

las medidas a nivel de dominio para aquellos casos en los que resulten proporcionadas.

4. **Realizar un piloto de objetivos de respuesta.** Probar objetivos por horas para registros maliciosos de propósito único y alta confianza, en lugar de declarar un plazo universal.
5. **Publicar datos de rendición de cuentas compatibles con la privacidad.** Utilizar un registro de transparencia por niveles con historiales firmados y pruebas restringidas.
6. **Evaluar el impacto causal.** No se debe equiparar una suspensión más rápida con un ahorro de dinero hasta que un estudio pre-registrado evalúe los efectos sobre las víctimas y el desplazamiento.

La conclusión constructiva no es que el problema original desaparezca una vez que se matizan sus afirmaciones. Es que ahora se pueden comprobar las afirmaciones centrales: el rango de daño tras la detección del 60-85 % es una hipótesis cuantitativa explícita; $100–150 es una hipótesis presupuestaria de ingeniería comprobable para una capa definida de sensores y triaje; y los objetivos de respuesta a escala horaria pueden ponerse a prueba para registros maliciosos de alta fiabilidad y con un único propósito. Publicar la carga de trabajo, los costes, las marcas de tiempo y los resultados, compararlos con una referencia y medir el desplazamiento y el error. La confirmación justificaría un cambio contractual y normativo; el rechazo identificaría qué hipótesis ha fallado.

Declaración editorial y sobre los métodos. PhishDestroy es un proyecto independiente y sin ánimo de lucro dedicado a la inteligencia sobre amenazas. Esta publicación es una propuesta de política y de ingeniería, no constituye asesoramiento jurídico, ni un programa de «ICANN», ni un artículo revisado por pares. Los rangos presupuestarios etiquetados como «modelos» son hipótesis de planificación. Las fuentes primarias de las afirmaciones se indican a continuación. Las correcciones pueden enviarse a través de los canales de contacto y de divulgación responsable del sitio web.

PERSPECTIVA EN PRIMERA PERSONA · LA RESPONSABILIDAD DEBE LIMITAR TANTO LA INACCIÓN COMO LA EXTRALIMITACIÓN

Un límite personal al poder de ejecución

No estoy pidiendo —ni quiero— acceso directo a una herramienta de bloqueo de dominios. Esa facultad requiere una revisión independiente, registros de auditoría públicos, un procedimiento de recurso rápido y la posibilidad de revocación.

Creo que hay muchas empresas competentes y responsables a las que se les podría confiar parte de este trabajo. A juzgar por mi experiencia y por lo que he publicado, no incluyo a NameSilo en ese grupo.

No aconsejaría a las empresas estadounidenses legítimas que confiaran funciones delicadas relacionadas con los abusos o la seguridad a contratistas concretos cuyos conflictos de intereses, competencia o conducta no puedan resistir un escrutinio independiente. Se trata de acciones documentadas, no de la nacionalidad: el origen ruso, por sí solo, no prueba nada, al igual que una dirección corporativa estadounidense tampoco prueba nada.

Quiero justicia y una rendición de cuentas efectiva en el caso de los registradores que obtuvieron ingresos por el registro y la renovación de dominios relacionados con campañas de estafa reiteradas. Cuando las pruebas apunten, más allá de la negligencia, a una posible complicidad consciente —ya sea mediante una participación operativa directa o actuando como intermediario informado cuya función consistía en mantener registrado y activo un dominio perjudicial a pesar de las repetidas advertencias—, dicha conducta debería ser objeto de una investigación independiente y, de confirmarse, acarrear consecuencias. No presento la sospecha como un hecho probado; pero la condición de intermediario no debe conferir inmunidad frente al escrutinio.

Revisar la investigación subyacente ↗

A

Referencias y notas bibliográficas

[1] **ICANN: presupuesto aprobado para el ejercicio fiscal 27 (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Fuente de la financiación operativa de 165,1 millones de dólares para el ejercicio fiscal 27 y composición de las fuentes de financiación.

[2] **ICANN: Enmienda Global de 2024 al Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Fuente contractual principal de las obligaciones de los registradores en materia de DNS Abuse.

[3] **ICANN: Enmienda global de 2024 al Base Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Fuente contractual principal de las obligaciones de mitigación del operador del registro.

[4] **Cumplimiento Contractual de ICANN: guía sobre obligaciones de DNS Abuse (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

Interpretación operativa, requisitos de los informes y ejemplos de mitigación adecuada.

[5] **ICANN: Aplicación de los requisitos de mitigación del DNS Abuse (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf

Informe semestral de aplicación y recuento de investigaciones y medidas de mitigación.

[6] **ICANN SSAC, SAC115: Informe sobre un enfoque interoperable para la gestión de abusos (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf

Contexto sobre la interoperabilidad de los informes de abuso y la calidad de las pruebas.

[7] **Hollenbeck, RFC 5731: Asignación de nombres de dominio mediante EPP (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html

Definición técnica de los valores de estado del dominio EPP, incluido el estado establecido por el servidor.

[8] **Laurie et al., RFC 9162: Certificate Transparency, versión 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html

Especificación autorizada del protocolo y límites de CT como sensor.

[9] **ICANN, Servicio centralizado de datos de zonas** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service

Ámbito de aplicación y modelo de acceso para los archivos de zona de los gTLD participantes.

[10] **Centro de Denuncias de Delitos en Internet del FBI, Informe anual 2025 del IC3** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Cifras de reclamaciones y pérdidas denunciadas, incluyendo el número de casos de phishing y spoofing.

[11] **Bijmans et al., «Catching Phishers By Their Bait» (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf

Mediciones específicas de cada conjunto de datos sobre la infraestructura de phishing y las duraciones observadas.

[12] **Dominios recién registrados y duración de las estafas de phishing, Revista de Ciberseguridad (2026)** · https://doi.org/10.1093/cybsec/tyag020

Datos empíricos recientes sobre los dominios de phishing recién registrados y la distribución de su vida útil.

[13] **Análisis inferencial de dominios registrados con fines maliciosos — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

Análisis financiado por ICANN sobre registros maliciosos y factores del ecosistema; limitaciones pertinentes para las afirmaciones causales.

[14] **Chainalysis, Tendencias en estafas con criptomonedas para 2026** · https://www.chainalysis.com/blog/crypto-scams-2026/

Estimación del proveedor sobre las entradas por estafas en la cadena de bloques en 2025; no se incluye en el total de phishing de dominios.

[15] **APWG, Informe sobre las tendencias de las actividades de phishing, primer trimestre de 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Ataques de phishing y URL detectados; estas cifras no equivalen al número de dominios únicos registrados.

[16] **Centro de Información sobre Delitos Informáticos / Interisle, Panorama del phishing en 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Distingue entre ataques observados, dominios únicos y dominios registrados con fines maliciosos.

[17] **Verisign, Informe sobre el sector de los nombres de dominio, segundo trimestre de 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Fuente de la cifra declarada de 401,6 millones de registros en todos los TLD.