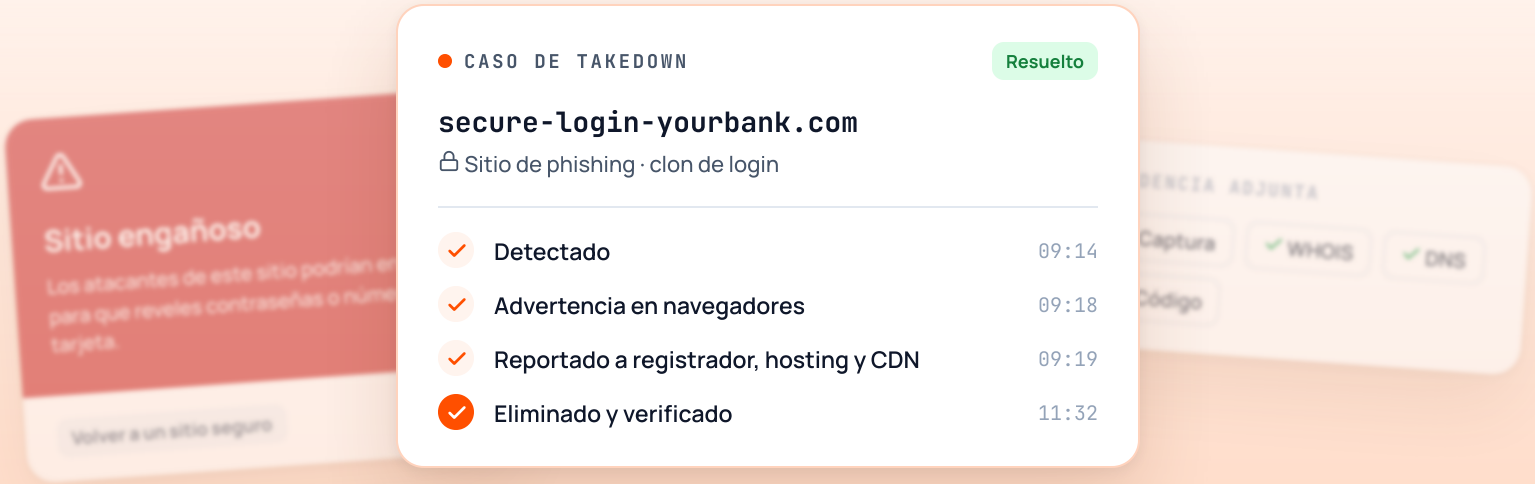
MANUAL DE TAKEDOWN DE PHISHING

Marcado en minutos. Eliminado en días.

Manual de takedown de phishing.

Los 14 pasos, un reporte para cada proveedor y qué hacer cuando nadie responde.



CONTENIDO

Qué incluye

Diez secciones, de los primeros minutos al informe final. Léelo una vez para armar tu proceso; durante un incidente, ten a mano las páginas 4, 8 y 9.

01 **Por qué decide la velocidad** p. 3
Dos relojes: tiempo hasta la advertencia y hasta la eliminación.

02 **Los 14 pasos** p. 4
Cada paso de un takedown y cuáles se pueden automatizar.

03 **Confirmar y capturar** p. 5
Asegúrate de que es phishing y regístralo antes de que cambie.

04 **Quién lo controla** p. 6
Registrador, hosting, CDN o plataforma: quién puede hacer qué.

05 **Primero, los navegadores** p. 7
Un reporte que protege a usuarios de Chrome, Safari y Firefox.

06 **Plantillas de reporte** p. 8
Versiones para registrador, hosting y CDN.

07 **Hostings difíciles** p. 10
Cloudflare, Vercel, Netlify y otras plataformas.

08 **Seguimiento y escalamiento** p. 11
Qué hacer cuando nadie responde.

09 **Elegir la vía** p. 12
Reportes de abuso, DMCA, URS y UDRP comparados.

10 **Medirlo** p. 13
Las cifras que muestran que los sitios realmente cayeron.

CUATRO FASES, CATORCE PASOS

01 **Confirmar**
Pasos 1–3

02 **Encontrar**
Pasos 4–6

03 **Reportar**
Pasos 7–11

04 **Cerrar**
Pasos 12–14

PARA QUIÉN ES

Equipos de seguridad, SOC y fraude que gestionan sitios de phishing que copian su marca, y las agencias y MSSP que lo hacen por ellos. Nada de esto requiere accesos especiales: cada vía está abierta a cualquier marca con evidencia.

SECCIÓN 01

01 Por qué decide la velocidad

La mayoría de los sitios de phishing hacen su daño en horas. Un takedown manual tarda días.

~60%

ACTIVOS MENOS DE 10 MINUTOS

de los dominios de phishing que ve Google existen menos de diez minutos. Cuando llega un takedown manual, la mayoría de las campañas ya se movieron.

Fuente: The Hacker News, marzo de 2024

Dos relojes, no uno

Un takedown tiene dos objetivos con distinta velocidad: la advertencia del navegador protege a la mayoría en horas; la eliminación termina el daño para todos. Mídelos por separado e inícialos al confirmar un sitio.

LA BRECHA, A ESCALA

Escala logarítmica



Fuentes: The Hacker News (2024), Cloudflare (2024), The Web Conference (2025), arXiv (2025). Referencias completas en la página 14.

REGLA PRÁCTICA

Nunca hagas los pasos en secuencia

Reporta a Google Safe Browsing y a cada proveedor el mismo día. Esperar al hosting antes de contactar al registrador le da tiempo al atacante para mover la página, y tu primer reporte se pierde.

SECCIÓN 02

02 Los 14 pasos

Cuatro fases. Casi todos los pasos son repetitivos, por eso la mayoría se puede automatizar.

01 Confirmar

¿Es phishing, está activo, qué datos recoge?

01 Confirmar que es phishing

Verificar que imita tu marca y recoge datos

Casi todo

02 Capturar evidencia

Capturas con fecha y hora, código, el señuelo

Automatizable

03 Revisar el cloaking

Cargarla desde un móvil, otros países y navegadores

Automatizable

02 Encontrar

¿Quién registró, aloja y protege el sitio?

04 Consultar el dominio

RDAP: registrador, contacto de abuso, fechas, DNS

Automatizable

05 Encontrar el hosting

Resolver la IP; buscar su dueño y contacto de abuso

Automatizable

06 Mirar detrás del proxy

Si hay un CDN delante, identificarlo y el origen

En parte

03 Reportar

A todos los que pueden advertir o eliminar, el mismo día

07 Navegadores

Google Safe Browsing y Microsoft SmartScreen

Automatizable

08 Registrador

Reporte de abuso con evidencia, pidiendo la suspensión

Automatizable

09 Hosting

La misma evidencia, pidiendo la eliminación

Automatizable

10 CDN o plataforma

Su formulario de abuso

Automatizable

11 El señuelo

El email, SMS, anuncio o red que lo envió

En parte

04 Cerrar

Eliminado en todas partes, y que no vuelva

12 Registrar tickets

Cada reporte, número de ticket y respuesta

Automatizable

13 Seguimiento y escalamiento

Insistir; escalar al registro, ICANN o CERT

Casi todo

14 Verificar y vigilar

Fuera de línea en todas partes; vigilar el mismo kit

Automatizable

LO QUE AÚN NECESITA UNA PERSONA

Casos inusuales (un sitio legítimo hackeado en lugar de uno falso), escalamientos que requieren una carta legal y decidir cuándo un dominio merece un UDRP.

SECCIÓN 03 · PASOS 1–3

03 Confirmar y capturar

Antes de reportar, asegúrate de que es phishing y regístralo. Las páginas de phishing cambian y desaparecen rápido.

Confirma tres cosas

1. **Imita tu marca:** tu nombre, logo, diseño o textos.
2. **Recoge algo:** una contraseña, un número de tarjeta, un código de un solo uso. Es la señal más clara de phishing.
3. **Está activa ahora,** tal como la verían tus clientes.

REVISA EL CLOAKING

Misma dirección, dos visitantes



Escritorio Un escáner o un visitante de escritorio no ve nada.

Móvil Una víctima en el móvil ve el login clonado.

Muchos kits de phishing muestran la página real solo a las posibles víctimas: un móvil, un visitante de un país, cualquiera que no sea un escáner conocido. Captura lo que ven las víctimas y aclara si solo aparece para algunos visitantes, o el revisor puede cerrar el reporte.

CAPTURA LA EVIDENCIA

Antes de que cambie

- La **URL completa** de la página, no solo el dominio
- El **código de la página**, o un archivo HAR
- **Tu página real**, para compararlas
- **Capturas** con fecha y hora en UTC
- El **señuelo**: SMS, email con encabezados, anuncio
- Cómo llegan las víctimas; cuándo se vio primero

Seguridad. Abre las páginas sospechosas en un navegador aislado o una máquina virtual, nunca en una laptop de trabajo, y nunca ingreses credenciales reales.

SECCIÓN 04 · PASOS 4–6

04 Quién lo controla

Un sitio de phishing suele involucrar a tres o cuatro empresas, y cada una puede hacer algo distinto.

ENTRE TU CLIENTE Y LA PÁGINA DE PHISHING

	QUÉ PUEDE HACER	CÓMO ENCONTRARLO
Navegadores Safe Browsing, SmartScreen	**Advertir** a los visitantes mientras llega la eliminación	Formularios de Google Safe Browsing y Microsoft SmartScreen
CDN o proxy p. ej. Cloudflare	**Reenviar** el reporte al hosting y al dueño; a veces advertir	La IP del sitio pertenece a un CDN: usa su formulario de abuso
Plataforma Vercel, Netlify, Shopify…	**Eliminar** el sitio de su plataforma	La dirección está en el dominio de la plataforma: su formulario de abuso
Hosting Dueño de la IP	**Eliminar** la página y cerrar la cuenta	El dueño de la IP en su registro regional (ARIN, RIPE, APNIC, LACNIC, AFRINIC)
Registrador Vendió el dominio	**Suspender** el dominio, para que ninguna página funcione	El registro RDAP del dominio: “Registrar Abuse Contact Email” (lookup.icann.org)

Si la IP pertenece a Cloudflare o un servicio similar, esa empresa no es el hosting: reenvía los reportes, así que reporta al CDN y, si puedes encontrarlo, directamente al hosting de origen. Proxies, servicios de privacidad y revendedores hacen que el primer contacto que encuentras no sea el que puede actuar.

WHOIS AHORA ES RDAP

Desde el 28 de enero de 2025, ICANN ya no exige a los registros de dominios genéricos operar el antiguo WHOIS; los datos de registro vienen de RDAP. El contacto de abuso del registrador sigue siendo público, aunque los datos del titular estén ocultos.

2,700+

DOMINIOS SUSPENDIDOS

Desde el 5 de abril de 2024, los registradores de dominios genéricos deben actuar con prontitud ante evidencia concreta de phishing. En los primeros seis meses, ICANN abrió 192 investigaciones bajo estas reglas, que llevaron a más de 2,700 suspensiones.

Fuente: ICANN, octubre de 2024

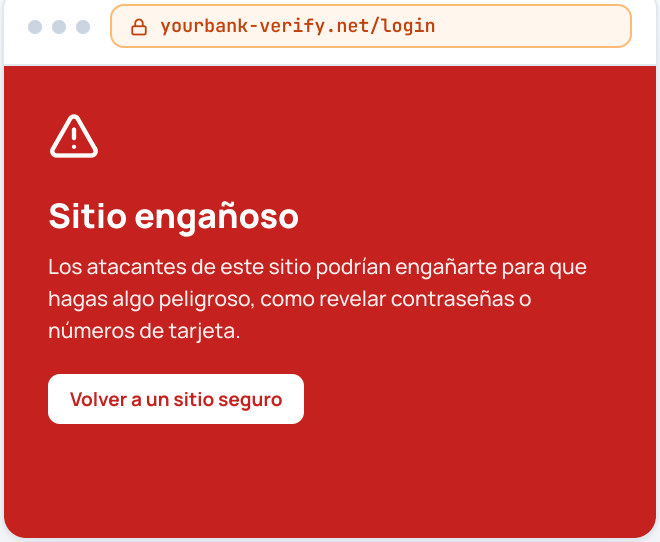
SECCIÓN 05 · PASO 7

05 Primero, los navegadores

Un reporte aceptado por Google Safe Browsing pone una advertencia en Chrome, Safari y Firefox, cerca del 88% de los navegadores en uso.

UN REPORTE, CASI TODOS LOS NAVEGADORES

Minutos a horas tras aceptarlo



NAVEGADORES QUE MUESTRAN LA ADVERTENCIA



~88% Edge, Opera, otros

Chrome	Google Safe Browsing
Safari	Google Safe Browsing*
Firefox	Google Safe Browsing
Edge	Microsoft SmartScreen
Opera	Listas propias, p. ej. PhishTank

Qué hace que acepten un reporte

- **La URL completa de la página de phishing,** no el dominio: la página de inicio puede parecer inofensiva.
- **Una página activa cuando el revisor la mira.** Si solo aparece en móvil o en un país, dilo.
- **Un formulario que recoge algo:** una contraseña, una tarjeta, un código de un solo uso.
- **Qué imita,** con la dirección de tu página real.
- **Una captura con fecha y hora,** por si la página cambia antes de la revisión.

⚠ **Una advertencia no es un takedown.** El sitio sigue en línea para quien use un navegador o una app que no consulta la lista, incluidos algunos navegadores dentro de apps. El atacante puede mover el kit a otra dirección, y la advertencia no lo sigue. Reporta para eliminarlo el mismo día. *Safari usa Tencent en equipos configurados para China continental; participación según StatCounter.

SECCIÓN 06 · PASOS 8–10

06 Plantillas de reporte

Envía la misma evidencia a todos a la vez. Las plantillas están en inglés, el idioma de los equipos de abuso. Reemplaza todo lo que esté entre ‹corchetes angulares›.

1. Registrador: pedir la suspensión

Nuevo mensaje · al contacto de abuso del registrador

```
1  Subject: Phishing on <domain> impersonating <Brand>: request to suspend

   To: <registrar abuse contact, from RDAP "Registrar Abuse Contact Email" or the
   registrar's abuse form>

   We are reporting a domain registered through you that is being used for
   phishing. It impersonates <Brand> (<official domain>) and collects
   <account passwords / card details / one-time codes> from our customers.

2  Phishing URL (full address):
     <https://domain/full/path>
     First seen: <YYYY-MM-DD HH:MM UTC>   Still live at: <YYYY-MM-DD HH:MM UTC>

   What it imitates:
     Our <login / checkout / support> page at <https://official URL>

3  Why it is phishing:
     - It copies our <name, logo, page layout and text>
     - It collects <what> through a form that sends the data to <where, if known>
     - It is being sent to our customers by <SMS / email / ads / social posts> (sample
   attached)

   Domain details:
     Registered: <date>   Nameservers: <ns1, ns2>   Resolves to: <IP> (<network owner,
   ASN>)

4  Evidence attached:
     1. Screenshot of the phishing page, <time UTC>
     2. Screenshot of our official page, for comparison
     3. <The lure message, with headers if it was an email>
     4. <Page source or HAR file>

5  Requested action:
     Please suspend <domain> under your abuse policy and your obligations to
     mitigate DNS abuse (phishing).

   We are <the brand owner / an authorized representative of Brand>.
   Contact: <name, role, email, phone>
```

1. **Un asunto que lo encamine**
   Dominio, marca y la acción que pides, para que llegue a la cola de abuso.
2. **La dirección completa**
   La página que recoge datos, con la hora en que se vio y sigue activa, en UTC.
3. **Por qué es phishing**
   Qué copia, qué recoge y cómo llegan las víctimas.
4. **Evidencia**
   Ambas capturas, el señuelo y el código de la página.
5. **Un pedido claro**
   La suspensión, citando su política de abuso y sus **obligaciones sobre abuso de DNS**.

SECCIÓN 06 · CONTINUACIÓN

2. Hosting: pedir la eliminación

Nuevo mensaje · al contacto de abuso del hosting

```
1  Subject: Phishing page hosted on your network (<IP>) impersonating <Brand>

   To: <host abuse contact, from the IP's RIR record "abuse-mailbox" / "OrgAbuseEmail",
   or the host's abuse form>

   A phishing page impersonating <Brand> is hosted on your network.

2  Phishing URL (full address):
     <https://domain/full/path>
     Server IP: <IP>   First seen: <time UTC>   Still live at: <time UTC>

   What it imitates / why it is phishing / evidence:
     <same as the registrar report>

3  Requested action:
     Please remove the phishing content and suspend the account responsible.
     Please keep logs, in case they are needed by law enforcement.

   Contact: <name, role, email, phone>
```

1. **Nombra la red**
   Indica que la página está en su red, con la IP.
2. **Dirección y servidor**
   La URL completa y la IP del servidor, para que encuentren la cuenta.
3. **Eliminar y guardar logs**
   Eliminación, suspensión de la cuenta y logs guardados para las autoridades.

3. CDN o proxy (por ejemplo, Cloudflare)

Usa el formulario de abuso del proveedor, elige la categoría de phishing, pega la URL completa y resume la evidencia en la descripción. Un CDN normalmente no guarda el sitio: reenvía tu reporte al hosting y al dueño, así que reporta también al hosting de origen si puedes identificarlo.

ANTES DE ENVIAR

- ✓ URL completa de la página, revisada de nuevo
- ✓ Qué datos recoge y cómo llegan las víctimas
- ✓ Reportado a Safe Browsing y SmartScreen
- ✓ Captura con fecha y hora (UTC), y nuestra página real
- ✓ Enviado al registrador, hosting y CDN al mismo tiempo
- ✓ Fecha de seguimiento definida

SECCIÓN 07

07 Hostings difíciles

Los proxies y las plataformas serverless cambian a quién reportas y qué le pides.

¿PROXY U HOSTING? CAMBIA EL PEDIDO

Un proxy delante



El proxy no guarda el sitio. Pídele que **reenvíe y advierta**, y reporta al hosting que está detrás.

La plataforma es el hosting



La plataforma ejecuta el sitio. Pídele que **elimine el deployment** y suspenda la cuenta.

PROVEEDOR	ROL	QUÉ PUEDE HACER	SI NO PASA NADA
Cloudflare (sitio con proxy)	Proxy	Reenviar al hosting y al dueño, dar su contacto, advertir	Reportar directo al hosting que indique; al registrador del dominio
Cloudflare Pages / Workers	Hosting	Eliminar el sitio	Seguimiento en el mismo reporte; Google Safe Browsing
Vercel	Hosting	Eliminar el deployment	Seguimiento; registrador si usa un dominio propio
Netlify, GitHub Pages	Hosting	Eliminar el sitio o el repositorio	Seguimiento; registrador si usa un dominio propio
Firebase Hosting (web.app)	Hosting	Eliminar el sitio	Google Safe Browsing

En un subdominio de plataforma como **acme-login-secure.vercel.app**, el dominio es de la plataforma: ningún registrador lo suspenderá y pedirlo retrasa tu reporte. Si tiene un dominio propio, repórtalo a su registrador.

QUÉ NECESITAN ESTOS PROVEEDORES

- **La URL completa**, con subdominio, que es el sitio
- **Prueba de que está activa:** captúrala justo antes de enviar
- **El pedido correcto:** eliminar, reenviar o suspender, según el rol

Mientras esperas. Hay hilos públicos de gente que esperó semanas por reportes a plataformas. Pon la dirección en Google Safe Browsing y SmartScreen el mismo día, para que los visitantes vean una advertencia mientras tanto.

SECCIÓN 08 · PASOS 11–14

08 Seguimiento y escalamiento

Aquí se van la mayoría de las horas: algunos proveedores actúan en horas, otros envían un acuse automático y nada más.

Cuando nadie responde

Al día siguiente — **Da seguimiento una vez**
En el mismo hilo, si la página sigue activa, con una captura nueva.

Después — **Sube un nivel**
El registro que administra la extensión (Verisign para .com) también tiene obligaciones sobre abuso de DNS.

Sin acción — **Queja ante ICANN**
Su equipo de Contractual Compliance acepta quejas sobre registradores que no actúan.

El mismo día — **Reporta a fuentes compartidas**
Los reportes al APWG llegan a muchas empresas de seguridad, registradores y hostings.

Persistente — **Involucra a tu CERT**
Sobre todo si el hosting está en otro país.

Lo que te responden

Respuestas de abuso — Abiertos 3 · Cerrados

RE	**Re: Phishing en yourbank-verify.net** `abuse@registrar.example` · Recibimos su reporte.	09:21	Automática
PR	**Reporte reenviado al hosting** `noreply@proxy.example` · No somos el proveedor de hosting.	09:24	Reenviado
HO	**Ticket 77120: contenido de phishing** `abuse@host.example` · Notificamos a nuestro cliente.	Día 2	Sigue activo
RE	**Re: [48213] Dominio suspendido** `abuse@registrar.example` · Se aplicó clientHold al dominio.	Día 3	Suspendido

Ilustrativo. Proveedores y dominios ficticios.

Reporta también el señuelo

El sitio necesita visitas. Reporta el canal que las envía: el proveedor de email, el remitente de SMS, la plataforma de anuncios o la red social que entregó el enlace. Detener el señuelo frena la campaña incluso antes de que caiga el sitio.

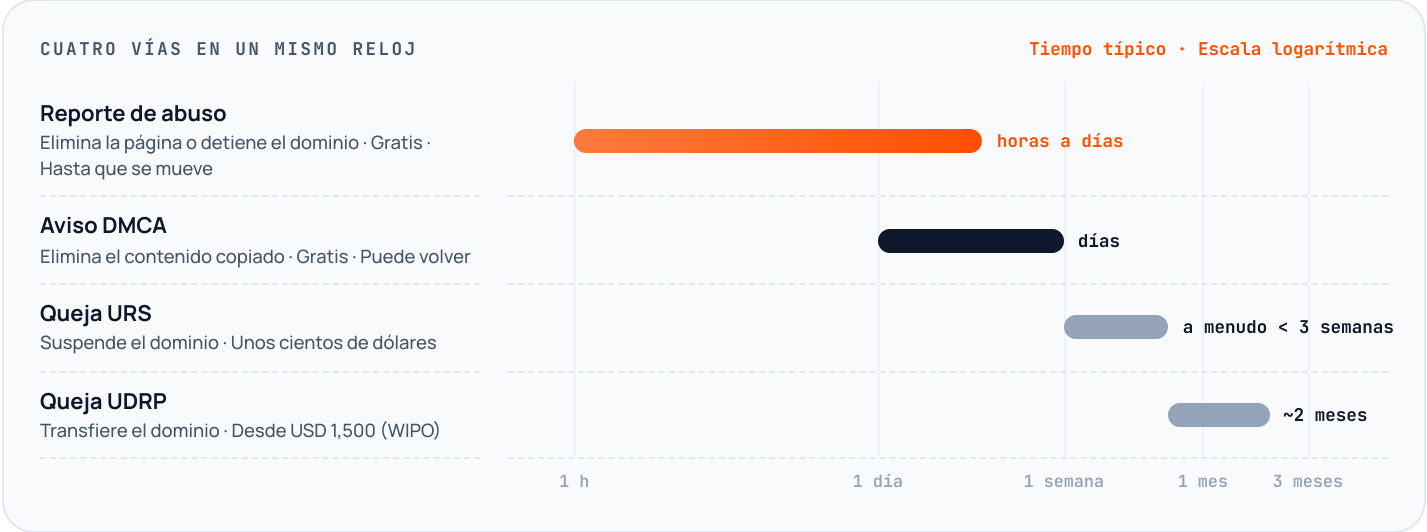
CIERRA BIEN EL CASO

- ✓ Fuera de línea en todas partes: cada URL, desde varios países y dispositivos
- ✓ Vigilando el mismo kit en dominios nuevos
- ✓ Evidencia y correspondencia guardadas con el caso
- ✓ Cerrado solo cuando se verifica la eliminación, no cuando se envió el reporte

SECCIÓN 09

09 Elegir la vía

Los reportes de abuso son la vía más rápida para un sitio de phishing activo. Un UDRP es la única que te da el dominio.



Qué vía para cada situación

SITUACIÓN	PRIMERO	LUEGO, SI HACE FALTA
Sitio de phishing activo en un dominio imitador	Reportes de abuso al hosting y registrador; Google Safe Browsing	UDRP si el dominio se reutiliza
Tu sitio copiado en un dominio sin relación	Reporte de abuso y aviso DMCA al hosting	Vigilar la misma copia
Página de phishing en un subdominio de plataforma	El formulario de abuso de la plataforma	Nada que disputar
Dominio imitador estacionado sin contenido	Monitorearlo por señales de activación	UDRP o URS si la mala fe es clara
Mala fe clara en un dominio genérico nuevo	URS para una suspensión rápida	UDRP para obtener el dominio

⚖ **No es asesoría legal.** Habla con tu abogado antes de presentar un UDRP, URS o DMCA. Usa las vías en paralelo, nunca en secuencia: envía los reportes de abuso el mismo día, y suma un UDRP solo si quieres el dominio.

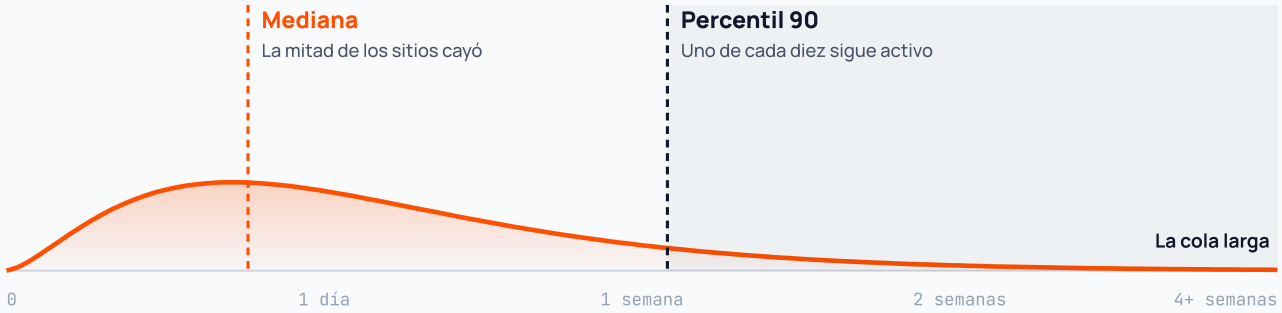
SECCIÓN 10

10 Medirlo

Mide amenazas eliminadas, no reportes enviados. Los promedios ocultan los sitios que duran semanas.

TIEMPO HASTA LA ELIMINACIÓN EN UN TRIMESTRE

Forma ilustrativa



MÉTRICA	CÓMO MEDIRLA	POR QUÉ IMPORTA
Tiempo hasta la advertencia	Confirmación → advertencia; mediana y percentil 90	Qué tan rápido se protege a la mayoría
Tiempo hasta la eliminación	Confirmación → fuera de línea, verificado; mediana y percentil 90	La cifra que termina el daño
Tasa de resolución	Casos fuera de línea y verificados, no “reportados”	Un caso estancado sigue robando datos
Tasa de reincidencia	El mismo kit u operador en un dominio nuevo	¿Campañas o sitios sueltos?
Horas de trabajo	Tiempo de analista por takedown, por fase	El costo de hacerlo a mano

Lo que no cuenta

- ✕ **Reportes enviados** o **takedowns solicitados:** un reporte no es una eliminación.
- ✕ **Alertas:** encontrar un sitio no protege a nadie hasta que se advierte y se elimina.
- ✕ **Un promedio solo:** uno de cada diez sitios activo durante semanas puede verse bien en la media.

DEFINE UNA LÍNEA BASE

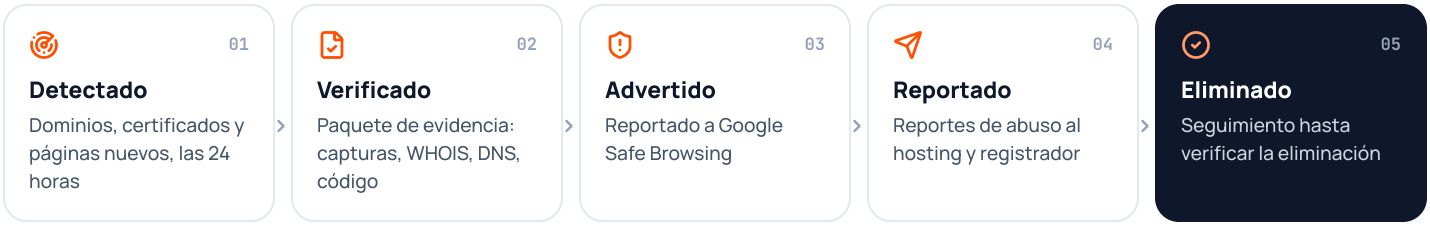
Mide tus próximos diez takedowns

Registra ambos relojes y las horas de trabajo. Así ves dónde se va el tiempo y qué automatizar primero.

CÓMO LO HACE SENTRIKE

El manual, ejecutado por agentes de IA

Sentrike ejecuta cada paso del takedown. Tu equipo puede seguir cada caso sin tener que hacer el trabajo.



Los agentes de IA de Sentrike confirman que el sitio es malicioso, arman el paquete de evidencia, lo reportan a Google Safe Browsing para que Chrome, Safari y Firefox adviertan a los visitantes en minutos, envían reportes de abuso al hosting y al registrador, y dan seguimiento hasta que el sitio está fuera de línea y se verifica la eliminación. La mayoría de los sitios se encuentra antes de que los clientes los reporten.

Deja de perseguir takedowns.

Mira los sitios de phishing que usan tu marca hoy, y qué tan rápido caen.

Solicitar acceso →

sentrike.ai/es/takedown

FUENTES

Google introduces enhanced real-time URL protection for Chrome (The Hacker News, 2024) thehackernews.com/2024/03/google-introduces-enhanced-real-time.html

“7 days later”: phishing site lifespan study (The Web Conference 2025) yonghwi-kwon.github.io/data/7_days_later_www25.pdf

Registration, Detection, and Deregistration: DNS abuse for phishing (arXiv, 2025) arxiv.org/pdf/2502.09549

Protecting Cloudflare sites from phishing (Cloudflare) blog.cloudflare.com/protecting-cloudflare-sites-from-phishing

2024 Global Amendments to the RAA and Registry Agreement (ICANN) www.icann.org/resources/pages/global-amendment-2024-en

ICANN’s DNS Abuse Mitigation Program: key updates from 2024 (ICANN) www.icann.org/en/blogs/details/icanns-dns-abuse-mitigation-program-key

RDAP in 2025: the practical successor to WHOIS (NameSilo) www.namesilo.com/blog/en/domain-names/rdap-in-2025-the-practical-succe

Browser market share worldwide (StatCounter) gs.statcounter.com/browser-market-share

Vercel community thread on a phishing report community.vercel.com/t/urgent-request-to-suspend-a-phishing-website-ho

WIPO domain name dispute fees www.wipo.int/en/web/amc/domain-name-disputes/fees