CSURFACE

WHITEPAPER · DIGITAL SUPPLY CHAIN

Riesgo en la cadena digital de proveedores · exposición heredada de terceros

Decenas de terceros ejecutan código en su aplicación — y no hay ninguna señal cuando uno de ellos cambia de dueño, es comprometido o expira. Mapear la cadena digital hasta tres niveles de profundidad convierte ese punto ciego en un inventario verificable.

CAPACIDAD Cadena Digital de Proveedores	PÚBLICO CISO · Riesgo · AppSec	EDICIÓN 2026
LECTURA 16 páginas	CLASIFICACIÓN Público	FUENTE Plataforma CSURFACE

RESUMEN EJECUTIVO

Su aplicación ejecuta código que no es suyo

La tesis de este whitepaper, en una página — lo que los ejecutivos necesitan saber antes del detalle técnico.

SITIOS AFECTADOS POR POLYFILL.IO

100 mil+

dominios servían el script malicioso sin saberlo

VULNERABILIDADES PROVENIENTES DE DEPENDENCIAS

80%

en apps web modernas, y no del código propio

PROFUNDIDAD DEL MAPEO CSURFACE

3 niveles

de la dependencia directa al subproveedor del subproveedor

En junio de 2024, el dominio **polyfill.io** — utilizado por más de 100 mil sitios para distribuir scripts JavaScript — pasó a inyectar código malicioso tras el cambio de titularidad. La mayor parte de las organizaciones afectadas desconocía esa dependencia. No existía vínculo contractual directo: Polyfill.io era subproveedor de un subproveedor, integrado al código años antes por equipos que ya no estaban en la organización.

El caso ejemplifica la norma. Las aplicaciones modernas ejecutan, en tiempo real, código que pertenece a decenas de terceros — **CDNs, scripts de analytics, APIs SaaS, bibliotecas con dependencias transitivas**. Cada uno de esos elementos es una puerta. Y la mayor parte de ellas no aparece en ningún inventario de proveedores.

Este whitepaper analiza el caso Polyfill.io como ejemplo arquetípico, recorre **otros incidentes públicos** detectables externamente (MageCart en British Airways, Ticketmaster vía Inbenta, Sea Turtle, subdomain takeover), construye **dos escenarios críticos** — toma de la cookie de sesión mediante subdomain takeover y *second-grade takeover* de dominio expirado — y presenta el enfoque de CSURFACE: el mapeo técnico y continuo de la cadena digital hasta **tres niveles de profundidad**, con diagramas prácticos en web y DNS y lecturas dedicadas a gestor, ingeniero y analista.

La tesis. Toda aplicación ejecuta código de terceros. Cada biblioteca, cada CDN y cada API integrada representa una dependencia heredada — sujeta a cambio de titularidad, compromiso o expiración sin notificación. Lo que no se mapea de forma continua no puede gestionarse ni defenderse.

Lo que cubre este whitepaper

- El caso Polyfill.io y tres incidentes públicos del mismo patrón.
- Los frentes técnicos — scripts, DNS, cabeceras y cookies.
- Dos escenarios críticos: cookie + subdomain takeover; second-grade takeover.
- El mapeo de CSURFACE en tres niveles y la lectura por perfil.

EL CASO POLYFILL.IO · PARTE 01

Un dominio cambió de dueño — y 100 mil sitios no lo notaron

La anatomía de un incidente público de cadena digital de proveedores, de la alerta ignorada al código malicioso.

Whitepaper 2026
CSURFACE

Qué ocurrió

Polyfill.io era una CDN de código abierto que distribuía "polyfills" — fragmentos de JavaScript destinados a proveer funcionalidades modernas en navegadores más antiguos. El servicio era gratuito y obtuvo amplia adopción en la comunidad de desarrollo web.

A comienzos de 2024, el dominio fue adquirido por un nuevo operador. El creador original del proyecto, Andrew Betts, **advirtió públicamente** que el dominio había cambiado de manos y ya no era confiable. La advertencia pasó desapercibida — porque no había monitoreo.

En junio de 2024, scripts maliciosos pasaron a ser servidos por el dominio: rastreo, redirecciones a sitios de apuestas y potencial robo de credenciales. Cloudflare y Google reaccionaron bloqueando el dominio en sus servicios — pero el daño ya se acumulaba desde hacía semanas.

Por qué el impacto fue tan amplio

1. **La dependencia era desconocida.** En muchos sitios el script había sido añadido años antes, por alguien que ya no estaba en la empresa. Era una dependencia invisible.
2. **La propiedad no era monitoreada.** No había proceso que siguiera los cambios de dueño de proveedores transitivos — exactamente el evento que disparó el ataque.
3. **CSP permisiva.** La mayoría de los sitios operaba sin una Content-Security-Policy restrictiva capaz de impedir la ejecución de un script alterado.
4. **SCA no cubría HTML/JS público.** Las herramientas de análisis de composición observaban dependencias de gestores de paquetes, no scripts cargados en tiempo de ejecución por el navegador.

La señal que faltó. El creador del proyecto comunicó públicamente que el dominio había cambiado de titularidad. La señal de alerta estaba disponible. La brecha fue la ausencia de un mecanismo capaz de monitorear cambios de propiedad en proveedores transitivos y encaminar ese aviso a los equipos de seguridad de las organizaciones consumidoras.

El patrón se repite. Polyfill.io ilustra un problema estructural que se repite en muchos proveedores digitales. Toda dependencia transitiva integrada sin monitoreo continuo representa un vector equivalente — sujeto a la misma cadena de eventos cuando el control de su titularidad cambia de manos.

CÓDIGO QUE NO ES SUYO · PARTE 02

La cadena digital tiene seis frentes — y casi ninguno se mapea

El problema general detrás del caso Polyfill.io: de qué está hecha la dependencia de terceros en una aplicación moderna.

87%
de las aplicaciones web modernas operan con 50 o más dependencias directas

80%
de las vulnerabilidades de una app web provienen de dependencias, no del código propio

94 días
es el tiempo medio hasta descubrir credenciales comprometidas en la cadena de proveedores

De qué se compone la dependencia

Las aplicaciones modernas ejecutan, en tiempo real, código que pertenece a decenas de terceros — y referencian, en el DNS, decenas de otros dominios externos. Ese riesgo se distribuye por **seis frentes técnicos** que una plataforma de ASM detecta desde el perímetro externo, sin agente ni instrumentación interna. De estos seis frentes, la confianza en DNS, el subdomain takeover, el WHOIS, los certificados y las credenciales de proveedor pertenecen a la superficie externa completa de la plataforma (ASM/Discovery); el módulo Supply Chain se concentra en la cadena de componentes embebidos — scripts, APIs y bibliotecas — mapeada hasta tres niveles de profundidad.

Cada frente sigue un patrón propio de adopción y de falla. Tratarlos con un único control — cuestionario, SCA o CSP aislada — es lo que produce la invisibilidad que Polyfill.io hizo pública.

El costo de la invisibilidad. Los ataques que explotan dispositivos de borde y VPNs gestionados por terceros crecieron cerca de ocho veces respecto al año anterior. Aproximadamente **el 30% de los breaches de 2025** involucró a un tercero — y el tiempo medio hasta el descubrimiento de credenciales comprometidas en la cadena de proveedores es de 94 días.

Fuentes: Snyk State of Open Source 2024; OWASP; Verizon DBIR 2025; IBM Cost of a Data Breach 2025 — informes públicos.

Las seis categorías de riesgo de la cadena digital

CRÍTICO **1 · JavaScript de terceros en el navegador**
Gestores de tags, scripts de analytics, A/B testing, polyfills, píxeles y widgets — cualquier código ejecutado en el navegador del cliente. Categoría de Polyfill.io y de la familia MageCart.

CRÍTICO **2 · Relaciones de confianza en DNS**
Registros SPF (y sus includes), MX y NS externos, CNAMEs apuntando a dominios de terceros, registros DKIM — la cadena de autoridad de su dominio principal.

ATENCIÓN **3 · Subdominios y recursos de nube referenciados**
CNAMEs apuntando a servicios de nube (AWS S3, Azure App Service, Heroku, GitHub Pages, Fastly) — superficie clásica de subdomain takeover cuando el recurso de origen queda desasignado.

ATENCIÓN **4 · APIs y endpoints llamados en runtime**
APIs SaaS, webhooks, píxeles de rastreo, endpoints de pago, integraciones de correo transaccional — toda llamada externa que la aplicación ejecuta en tiempo real.

ATENCIÓN **5 · Cabeceras y protecciones HTTP**
CSP, SRI, CORS, HSTS, flags de cookie (Secure, HttpOnly, SameSite) — la postura técnica que decide el desenlace cuando uno de los terceros anteriores es comprometido.

CRÍTICO **6 · Dominios en estado degradado**
Expiración próxima, cambio reciente de WHOIS, transferencia de operador, certificado en renovación atípica — señales anticipadas de takeover o second-grade en la cadena.

OTROS CASOS REALES · PARTE 03 · SCRIPTS Y CDN

Polyfill.io no fue el primero

Tres incidentes públicos anteriores que siguieron el mismo patrón — un tercero embebido en la cadena digital, comprometido sin aviso a la organización consumidora.

El patrón detrás de los casos. En ambos incidentes a continuación, el ataque entró por un componente que la organización objetivo había integrado años antes, sin mecanismo posterior de monitoreo. El vector difiere — script directo en la página de pago o compromiso de un proveedor entero de widget —, pero la estructura es la misma, y la detección externa es equivalente: el renderizado headless de la página identifica cualquier cambio en el contenido entregado por el tercero.

British Airways · MageCart (2018)

Entre el 21 de agosto y el 5 de septiembre de 2018, atacantes inyectaron **22 líneas de JavaScript** en la página de pago del sitio y de la aplicación de British Airways. El script capturaba número de tarjeta, nombre, dirección y CVV en tiempo real y los enviaba a un servidor controlado por terceros. La inyección partió de la cadena digital: un componente JavaScript de proveedor ya integrado al sitio fue modificado para incluir el skimmer, sin alteración visible para el equipo interno.

El ataque duró aproximadamente **15 días** antes de ser detectado. Cerca de **380.000 transacciones** fueron comprometidas.

Impacto. Multa de **£20 millones** por el ICO bajo GDPR (2020) — inicialmente propuesta en £183 millones. Compensaciones civiles a clientes, daño reputacional duradero. El regulador señaló la ausencia de monitoreo técnico del JavaScript de terceros como falla central de la empresa.

Ticketmaster · vía Inbenta (2018)

En **junio de 2018**, Ticketmaster divulgó que las páginas de pago de sus sitios estaban sirviendo un script malicioso desde hacía aproximadamente nueve meses. El script no estaba embebido directamente en el código de Ticketmaster: era servido por el widget de chat de atención de **Inbenta**, proveedor integrado a las páginas de pago.

Inbenta confirmó el compromiso de su infraestructura. El JavaScript que alojaba — cargado en tiempo real por el navegador desde el origen legítimo del proveedor — fue alterado para incluir un skimmer. Aproximadamente **40.000 clientes** tuvieron sus datos expuestos.

Impacto. Multa de **£1,25 millones** por el ICO. Vector distinto al del caso BA: lo que fue comprometido fue un **proveedor entero** de aplicación, no el código de Ticketmaster. El JavaScript cargado por el navegador seguía viniendo del origen legítimo del proveedor — con toda la confianza de cadena heredada.

Cómo CSURFACE detecta esta categoría

La categoría de scripts y CDN es la más visible externamente — y la mejor cubierta por el **renderizado headless**. La plataforma carga cada página de la organización como un navegador real, registra todo JavaScript de origen externo ejecutado, calcula el hash de cada archivo recibido y lo compara con la baseline.

Para cada script de tercero identificado, CSURFACE mantiene: el origen (dominio y CDN), el WHOIS actual, el hash del contenido entregado y el histórico de cambios. Cualquier alteración — dominio que cambia de dueño, hash que cambia, CDN que redirige — genera una alerta en hasta **24 horas**.

Resultado. Los dos incidentes de esta página serían detectados antes del impacto material — el caso BA, por la detección de la inyección en el JavaScript de la página de pago; el de Ticketmaster/Inbenta, por el cambio de hash en el script cargado desde el origen del proveedor.

OTROS CASOS REALES · PARTE 03 · DNS, MX Y DOMINIOS

La cadena digital también vive en el DNS

Subdominios apuntando a recursos abandonados, proveedores de DNS comprometidos, registros huérfanos — una clase de riesgo que no aparece en ningún repositorio de código.

Whitepaper 2026
CSURFACE

Dónde reside el riesgo en el DNS. Las aplicaciones modernas dependen de decenas de nombres — subdominios propios, registros que apuntan a servicios de nube, proveedores externos de DNS y correo, includes de SPF. Cada uno de esos nombres es, en sí, un nodo de la cadena digital. Cuando el control de uno de ellos se pierde — porque el recurso fue desasignado, el dominio expiró o el proveedor fue comprometido —, la confianza que apuntaba a él sigue siendo válida, pero ahora sirve a quien asuma el control.

Subdomain takeover mediante CNAME huérfano

El patrón más común: un subdominio de la organización — por ejemplo, **blog.empresa.com.br** — apunta, mediante registro CNAME, a un servicio de nube (Heroku, AWS S3, GitHub Pages, Azure App Service). El servicio fue desasignado en algún momento, pero el CNAME permaneció. Cualquier persona puede entonces recrear el recurso de nube con el mismo nombre, y el subdominio pasa a servir su contenido — bajo el nombre de confianza de la organización.

Documentado en cientos de reportes públicos en HackerOne, con casos de Microsoft, Uber, Shopify, Starbucks y múltiples organizaciones de gran porte. Los recursos abandonados en **Azure, AWS, Heroku, GitHub Pages y Fastly** son los más frecuentemente afectados.

Impacto. Phishing autenticado bajo dominio real, distribución de malware bajo HTTPS válido, robo de cookies en dominios hermanos (ver escenario hipotético, página 8). Detectado típicamente solo tras su explotación por investigadores o atacantes.

Sea Turtle · secuestro de DNS upstream (2017-2019)

Campaña de Estado-nación documentada por Cisco Talos. Los atacantes comprometieron **proveedores de DNS** en al menos 13 países — sobre todo en Oriente Medio y el Norte de África — y modificaron registros NS y A de organizaciones objetivo: gobiernos, empresas de energía, agencias de inteligencia. Con el DNS secuestrado, redirigieron el tráfico a infraestructura controlada por ellos y emitieron certificados TLS válidos bajo los nombres de las víctimas, permitiendo la captura de credenciales en sesiones aparentemente legítimas.

Más de **40 organizaciones** en 13 países fueron identificadas como objetivo directo.

Impacto. Captura silenciosa de credenciales y tráfico de organizaciones estratégicas; compromiso de cadenas enteras de correo oficial; uso de certificados válidos para evitar la detección por TLS pinning o inspección manual.

MX y SPF apuntando a dominios huérfanos

Variación menos visible, pero común: registros **MX** o includes de **SPF** de la organización — o de proveedores integrados — apuntan a dominios de terceros que fueron desactivados o expiraron. El registro sigue publicado y válido. Si el dominio es re-registrado por un atacante, este pasa a ser un origen autorizado para recibir correos (MX) o para enviar correos autenticados en nombre de la organización (SPF include).

El caso bancario detallado en la **página 9** es la manifestación más grave de ese patrón — un SPF include apuntando a dominio de proveedor de e-mail marketing expirado.

Impacto. Recepción de correo destinado al subdominio huérfano (recuperación de contraseña, facturas, comunicaciones de proveedor); o envío de phishing masivo autenticado por SPF como si fuera la organización legítima — abordado en detalle en la próxima sección.

OTROS CASOS REALES · PARTE 03 · HEADERS Y PROTECCIONES

Lo que la aplicación permite importa tanto como lo que carga

Cuatro configuraciones de cabecera y cookie cuya ausencia o permisividad determina si el navegador resistirá o amplificará un ataque de cadena.

Por qué existe esta sección. Las tres páginas anteriores trataron de lo que está en la cadena digital — scripts, dependencias, registros DNS. Esta página trata de las protecciones del navegador que deciden el desenlace cuando uno de esos elementos es comprometido. En casi todos los casos públicos, una protección bien configurada habría reducido significativamente el impacto o bloqueado la explotación.

Content-Security-Policy permisiva o ausente

La CSP define, en la cabecera HTTP, qué orígenes pueden cargar scripts, estilos y conexiones. Una política restrictiva impide la ejecución de scripts de orígenes no autorizados; una permisiva (con wildcards o `unsafe-inline`) o ausente deja al navegador aceptar cualquier script.

La CSP protege contra la **inyección de orígenes nuevos** — XSS, o un proveedor sirviendo desde un origen inédito. **No** protege, en cambio, cuando el origen ya autorizado es, él mismo, comprometido (caso Polyfill.io). Para ese escenario, la defensa directa es el **SRI**, en el bloque contiguo.

Impacto. Sin CSP restrictiva, cualquier script de cualquier origen se ejecuta. Un único componente comprometido en la cadena digital obtiene control total de la página — lectura de formularios, exfiltración de cookies no-HttpOnly, redirección.

CORS con wildcard u origen reflejado

La cabecera `Access-Control-Allow-Origin` determina qué orígenes pueden leer respuestas de una API autenticada. Configurada con `*` o reflejando dinámicamente el origen de la solicitud (sin validación), permite que cualquier sitio externo ejecute solicitudes autenticadas en nombre del usuario logueado — siempre que el navegador envíe cookies — y lea el resultado.

Ese patrón amplifica ataques de cadena: un script comprometido en cualquier origen puede leer datos sensibles de la API de la organización objetivo, incluso cuando está alojado en otro dominio.

Impacto. Fuga de datos autenticados — saldos, historiales, perfiles — hacia cualquier origen que ejecute código en el navegador del usuario, incluidos orígenes de la cadena digital comprometidos.

Subresource Integrity (SRI) ausente

SRI es un atributo HTML que carga, junto a la etiqueta `<script src="...">`, un hash criptográfico del contenido esperado. El navegador calcula el hash del archivo recibido y lo compara antes de ejecutar. Si el contenido del servidor de origen cambió — porque la CDN fue alterada, comprometida o sustituida —, el navegador rechaza la ejecución.

Sin SRI, el navegador acepta cualquier contenido que el servidor de la CDN devuelva. Un swap como el de Polyfill.io pasa silenciosamente.

Impacto. La alteración de un archivo en la CDN — deliberadamente o por compromiso del proveedor — se ejecuta sin ninguna señal de aviso. SRI es la defensa criptográfica directa contra la categoría de riesgo de Polyfill.io.

Cookies sin flags de protección

Las cookies de sesión deben configurarse con tres flags: **Secure** (solo HTTPS), **HttpOnly** (no accesible vía JavaScript) y **SameSite** (Lax o Strict — restringe el envío en solicitudes entre sitios). La ausencia de cualquiera de ellas amplía el impacto de un compromiso en la cadena digital.

HttpOnly, en particular, es la defensa crítica contra la captura mediante JavaScript inyectado — un vector común en todos los casos de la página 5. Su ausencia transforma un XSS o un script comprometido en toma de cuenta directa.

Impacto. Sin HttpOnly, cualquier script de la cadena digital — legítimo o comprometido — puede leer la cookie de sesión y enviarla a un endpoint controlado por el atacante. Es el vector central del escenario hipotético de la próxima página.

ESCENARIOS CRÍTICOS · PARTE 04 · ESCENARIO 01

Subdomain takeover + cookie emitida para el parent domain

Cómo un subdominio olvidado apuntando a un recurso de nube desasignado se transforma en toma de cuenta a escala — sin alerta, sin MFA, sin rastro fácil.

Whitepaper 2026
CSURFACE

El escenario. Una institución financiera opera **app.banco.com.br** como aplicación crítica, con autenticación y MFA. Para soportar single sign-on entre servicios internos, la **cookie de sesión se emite para el parent domain** — `Domain=.banco.com.br`. La organización opera decenas de subdominios; uno de ellos — una página promocional de campaña cerrada en 2022 — apunta, mediante CNAME, a un bucket de nube que fue desasignado. El registro DNS permaneció publicado.

La cadena de eventos del ataque

1. **Reconocimiento.** El atacante enumera subdominios públicos de `banco.com.br` e identifica `promo2022.banco.com.br` apuntando, mediante CNAME, a un bucket de nube cuyo nombre no está registrado. El subdominio es elegible para takeover.
2. **Toma del recurso.** El atacante registra el bucket con el mismo nombre en el proveedor de nube. El CNAME existente pasa a resolver hacia infraestructura controlada por él. El subdominio se sirve bajo HTTPS válido — el proveedor emite certificado para el nombre solicitado.
3. **Publicación del payload.** El atacante aloja en el bucket una página HTML simple con un script de captura — lectura de `document.cookie` y envío al endpoint del atacante vía `fetch()`. Como la víctima visitará un subdominio de `banco.com.br`, el navegador adjuntará la cookie emitida para `.banco.com.br`.
4. **Atracción de la víctima.** El enlace `promo2022.banco.com.br` todavía aparece en correos de marketing antiguos, materiales archivados, redirects internos no revocados y en respuestas indexadas en motores de búsqueda. Basta con que una fracción de las víctimas haga clic para que el ataque tenga escala material.
5. **Captura y abuso.** El navegador de la víctima — ya autenticado en `app.banco.com.br` en otra pestaña — envía la cookie de sesión al subdominio comprometido. Si la cookie no tiene **HttpOnly**, el JavaScript del atacante la lee y la exfiltra. El atacante se autentica en `app.banco.com.br` usando la cookie capturada — **después del MFA, porque la sesión ya está establecida**.

Por qué este escenario es particularmente grave. El atacante opera *después* del MFA — la sesión capturada ya está autenticada. La solicitud parte de la IP de la víctima o de una IP similar, lo que dificulta la detección por SIEM. El subdominio comprometido tiene HTTPS válido y nombre real de la organización. Y el vector es silencioso: ningún log de la aplicación principal muestra la captura — ocurre en un subdominio fuera del monitoreo.

Las tres condiciones simultáneas

El escenario solo funciona cuando tres condiciones coexisten en la organización:

1. Un subdominio huérfano apuntando a recurso de nube desasignado — disponible para takeover.

2. Cookie de sesión emitida para el parent domain — adjuntada a todos los subdominios.

3. Cookie sin flag HttpOnly — legible por JavaScript en el navegador.

Cada condición, de forma aislada, es una decisión técnica defendible en algún contexto. La composición de las tres es la vulnerabilidad — y ningún análisis de aplicación aislado la ve.

Cómo lo detecta CSURFACE. El descubrimiento continuo mapea todos los subdominios públicos de la organización; la inspección identifica CNAMEs apuntando a recursos desasignados (subdomain takeover); el análisis headless registra el alcance y las flags de las cookies de la aplicación principal. Las tres condiciones generan una única alerta crítica, antes de que el atacante llegue primero.

ESCENARIOS CRÍTICOS · PARTE 04 · ESCENARIO 02

Second-grade takeover · cuando el dominio del proveedor expira

El takeover de primer grado alcanza un subdominio propio. El de segundo grado alcanza un dominio entero de la cadena — generalmente de un proveedor — que expiró y fue re-registrado. Toda confianza heredada pasa, sin alarma, al nuevo dueño.

Whitepaper 2026
CSURFACE

El concepto. Un dominio de tercero — proveedor de e-mail marketing, socio de campaña, CDN, integrador cerrado — expira por falta de renovación, cese de operación, divestiture en M&A o simple olvido. La organización consumidora, sin embargo, mantiene registros DNS, includes de SPF, CNAMEs y referencias de scripts apuntando a ese dominio. El dominio es re-registrado por un atacante. Toda la confianza heredada — autenticación SPF, ejecución de script, recepción de correo — pasa instantáneamente al nuevo controlador, sin ninguna alarma técnica por parte de la organización.

El caso · banco con SPF autorizando dominio de proveedor ya expirado

Un banco contrató, en 2018, un proveedor de e-mail marketing — `envio-camp.com.br` — para disparar comunicaciones transaccionales y promocionales. Para que esos mensajes pasaran por los filtros anti-spam, el banco incluyó el dominio del proveedor en su registro SPF:

```
v=spf1 include:_spf.envio-camp.com.br include:_spf.outras.com.br ~all
```

Años después, el proveedor cesó su operación. El include, sin embargo, permaneció en el SPF del banco — el dominio no constaba en ningún inventario de proveedores activos, y el contenido del registro no se revisaba.

En los **primeros días de operación** de CSURFACE en el banco, el mapeo de la cadena de dominios referenciados en la configuración externa identificó que `envio-camp.com.br` **ya estaba expirado** — el dominio autorizado por el include del SPF se encontraba, en ese momento, libre para registro público por cualquier parte. La alerta fue escalada al equipo de seguridad, que removió el include del SPF antes de que un tercero re-registrara el dominio. **El vector fue neutralizado antes de poder ser explotado.**

Lo que estaría en riesgo sin la detección. Con el include activo y el dominio re-registrado por un tercero, el atacante publicaría `_spf.envio-camp.com.br` autorizando sus propias IPs y enviaría correos autenticados por SPF como si fuera el banco. Los filtros anti-spam los aceptarían — SPF pasa, IP autorizada. Cientos de miles de correos de phishing autenticados podrían entregarse a los clientes del banco; robo de credenciales a escala; exposición regulatoria ante el BACEN y la ANPD (RGPD). La señal — la expiración del dominio en la cadena — estuvo pública por más de un año. Fue exactamente esa señal la que la plataforma capturó.

Otras variaciones del mismo patrón

CNAME hacia dominio expirado. Un subdominio apunta a `cdn-do-fornecedor.com`, proveedor que cerró en 2021. El dominio expira; el atacante lo registra y pasa a servir scripts o páginas bajo el nombre de la organización cliente.

MX hacia dominio expirado. Un subdominio (`fatura.empresa.com.br`) tiene registro MX apuntando a servidor de proveedor extinto. El atacante registra el dominio y recibe los correos dirigidos a ese subdominio — incluidos recuperación de contraseña, facturas y comunicaciones de proveedores.

Script src hacia dominio expirado. Páginas heredadas cargan, mediante `<script src>`, un archivo de un dominio que ya no existe. El atacante registra el dominio y ejecuta código bajo el nombre de confianza de la página anfitriona — vector equivalente al de Polyfill.io.

DKIM huérfano. Un registro DKIM apuntando a clave pública en dominio extinto puede ser secuestrado, permitiendo al atacante firmar correos como si fuera la organización legítima.

Cómo lo detecta CSURFACE. La plataforma monitorea continuamente todos los dominios referenciados en la configuración externa de la organización — incluidos includes de SPF, MX, CNAMEs, NS y referencias en scripts. Para cada uno, observa el estado de registro, la fecha de expiración y los cambios de propiedad en el WHOIS. La expiración inminente — o consumada — de un dominio en la cadena es alerta crítica, llevada a los equipos antes de que el re-registro sea posible.

POR QUÉ EL ENFOQUE TRADICIONAL FALLA · PARTE 03

El cuestionario no ve código

Por qué los enfoques tradicionales de TPRM y SCA cubren el contrato — y dejan fuera el riesgo técnico real.

Tres brechas de los enfoques tradicionales

Los cuestionarios de proveedores no ven código. La gestión de riesgo de terceros (TPRM) tradicional evalúa a los proveedores mediante cuestionarios autodeclarados. Eso atiende requisitos de cumplimiento, pero dice poco sobre el riesgo real: no se completa un cuestionario sobre cada una de las decenas de dependencias de npm de una aplicación.

SAST y SCA tradicionales solo observan el código propio y las dependencias de gestor de paquetes. No perciben el JavaScript inyectado en tiempo de ejecución por un gestor de tags, no ven la CDN externa que sirve un archivo crítico y no siguen los cambios de propiedad de dominio.

La CSP es una defensa; el diagnóstico exige una inspección aparte. Una Content-Security-Policy bien configurada impide scripts no listados. Pero la mayoría de los sitios comienza con una política permisiva y nunca la restringe — y la CSP, por sí sola, no revela qué scripts carga realmente la aplicación.

La brecha común. Ninguno de los enfoques tradicionales fue concebido para inspeccionar lo que la aplicación ejecuta en tiempo real, ni para monitorear de forma continua la postura y la titularidad de los proveedores tras la formalización de los contratos.

Dónde se detiene cada enfoque

LO QUE NECESITA VERSE	TPRM / SCA TRADICIONAL	MAPEO CSURFACE
JavaScript cargado en runtime	No cubre	**Renderizado headless**
CDN externa de archivo crítico	No cubre	**Mapeada por inspección**
Cambio de propiedad de dominio	No cubre	**Alerta de WHOIS**
Dependencias transitivas más allá del N1	Parcial	**Tres niveles**
Postura externa real del proveedor	Autodeclarada	**Verificada externamente**
Frecuencia de la evaluación	Puntual / anual	**Continua**

El resultado práctico. La organización mantiene un repositorio de cuestionarios completados y un indicador formal de cumplimiento — mientras las dependencias técnicas de mayor riesgo jamás fueron inspeccionadas y permanecen sin monitoreo tras la formalización de los contratos.

MAPEO EN 3 NIVELES · PARTE 04

De la dependencia directa al subproveedor del subproveedor

El enfoque de CSURFACE: tres niveles de profundidad técnica, mapeados y monitoreados continuamente.

Whitepaper 2026
CSURFACE

LA CADENA DIGITAL, DESPLEGADA · TRES NIVELES DE PROFUNDIDAD TÉCNICA

1

N1 · Dependencias directas

Para cada activo descubierto, la plataforma identifica el JavaScript cargado en tiempo de ejecución mediante análisis headless, los manifiestos de paquete en repositorios públicos, las APIs llamadas en runtime y los webhooks recibidos.

2

N2 · Subproveedores

Para cada proveedor de Nivel 1, CSURFACE mapea sus dependencias: qué CDNs usa, qué APIs llama y dónde aloja la infraestructura. La dependencia transitiva de una biblioteca también se despliega aquí.

3

N3 · Subproveedor del subproveedor

La profundidad máxima que permiten los datos públicos — el punto donde estaba Polyfill.io: el operador del dominio, la IP y la CDN que de hecho sirven el código al navegador del usuario.

NIVEL 1 · DEPENDENCIA DIRECTA

Su aplicación
contrata al proveedor de marketing

El contrato que la organización conoce y que aparece en el inventario de proveedores.

NIVEL 2 · SUBPROVEEDOR

Proveedor de marketing
embebe el script de polyfill en la página

La dependencia heredada — añadida por terceros, sin contrato directo con la organización.

NIVEL 3 · SUBPROVEEDOR DEL SUBPROVEEDOR

polyfill.io
dominio operado por un tercero · IP y CDN desconocidos

El nodo que cambió de dueño y pasó a servir código malicioso — invisible hasta que la cadena se despliega.

Señales monitoreadas continuamente · para cada nodo de la cadena

CRÍTICO **Cambios de propiedad (WHOIS)**
Alerta cuando un dominio de la cadena cambia de dueño — la señal exacta que faltó en el caso Polyfill.io.

ATENCIÓN **Postura externa del proveedor**
Vulnerabilidades y configuraciones expuestas en el perímetro de cada nodo de la cadena.

ATENCIÓN **Cambios de DNS**
Alteraciones en registros NS, MX y A que indiquen redirección de infraestructura.

CRÍTICO **Credenciales filtradas**
Credenciales del proveedor a la venta o expuestas en foros y repositorios públicos.

ATENCIÓN **Certificados**
Renovaciones, cambio de emisor y proximidad de expiración de cada certificado.

CRÍTICO **Divulgaciones de incidente**
Anuncios públicos de compromiso del propio proveedor.

El análisis headless ejecuta el renderizado completo de la página, incluyendo scripts dinámicos; el monitoreo opera de forma continua, sin agente instalado en el entorno del cliente.

MAPEO EN 3 NIVELES · PARTE 05 · DIAGRAMAS

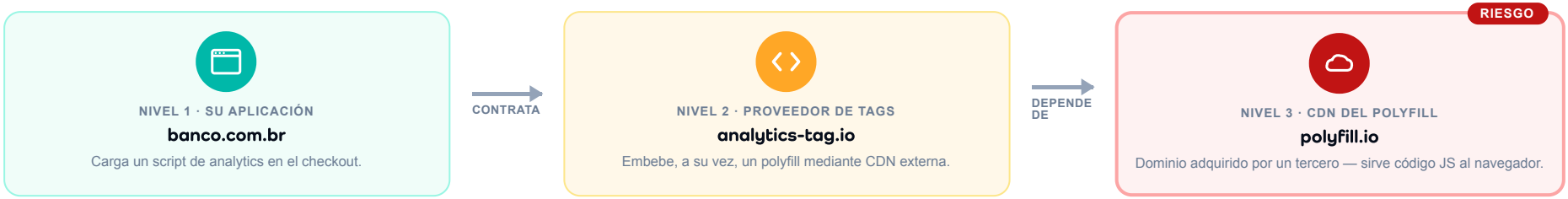
Dos diagramas prácticos · web y DNS

La misma estructura de tres niveles aplicada a dos categorías distintas — código de página y registro de correo. En ambas, el riesgo vive en el tercer nivel.

Whitepaper 2026
CSURFACE

El patrón es estructural y vale para cualquier categoría de proveedor. En ambos ejemplos, la organización contrata un proveedor de Nivel 1, este proveedor depende, a su vez, de un Nivel 2, y el riesgo real surge en un Nivel 3 no mapeado por la organización — pero que decide el desenlace.

EJEMPLO 01 · CADENA DE SCRIPTS EN EL NAVEGADOR



EJEMPLO 02 · CADENA DE AUTORIDAD DEL CORREO (SPF)

Dónde detecta CSURFACE este patrón. El descubrimiento continuo mapea ambas cadenas — JavaScript en runtime (renderizado headless) y dominios en configuración externa (SPF includes, CNAME, MX, NS, scripts src). Para cada nodo en los tres niveles, la plataforma observa el estado de registro, la titularidad en el WHOIS, los cambios de DNS y las variaciones de contenido. La señal — cambio de propiedad, expiración inminente, alteración de hash — llega al equipo antes de la explotación.

LECTURA POR PERFIL · PARTE 06

La misma cadena digital, tres cortes diferentes

Gestores, ingenieros y analistas necesitan cortes distintos del mismo dato para decidir, configurar y responder a amenazas en la cadena digital de proveedores.

Por qué existen tres cortes. El riesgo de cadena digital atraviesa tres capas organizacionales con horizontes diferentes — capital, configuración y operación. El **gestor** necesita el número agregado en moneda para deliberar y rendir cuentas; el **ingeniero** necesita el detalle técnico para corregir; el **analista** necesita el contexto y los indicadores para responder en tiempo real. Sin esa segmentación, el mismo informe atiende mal a los tres.

Para el gestor · CISO, gerente de riesgo

Lo que importa. Exposición financiera agregada, adherencia al apetito de riesgo aprobado, cumplimiento de normas aplicables (BACEN, RGPD, NIS2, PCI DSS) y métricas de cobertura — cuántos proveedores están bajo monitoreo, cuántas alertas críticas están abiertas, cuánto tiempo llevó de la detección a la resolución.

Lo que recibe de CSURFACE. Panel ejecutivo con inventario consolidado de proveedores en tres niveles, alertas críticas abiertas, comparación con el apetito, evidencia auditable para el comité. Informes periódicos que pueden presentarse al consejo sin traducción técnica adicional.

Cómo actúa. Aprueba inversión de remediación con base en el trade-off de reducción de exposición. Comunica la posición de la organización al consejo, al regulador y al auditor con datos verificables. Compara la postura interna con la de pares del sector.

Para el ingeniero · AppSec, DevSecOps

Lo que importa. Detalles técnicos completos del hallazgo — qué script fue alterado, qué hash cambió, qué subdominio apunta a qué recurso desasignado, qué SPF include referencia qué dominio expirado. El vector de explotación, el contexto en la arquitectura y el camino de remediación.

Lo que recibe de CSURFACE. Alertas técnicas con contexto completo — dominio afectado, recurso de origen, evidencia del cambio (hash antes/después, WHOIS antes/después), integración con pipelines de CI/CD y ticketing. Recomendación de corrección concreta para cada categoría.

Cómo actúa. Remueve la dependencia problemática, configura CSP restrictiva y SRI en los scripts críticos, actualiza registros SPF, retira CNAMEs huérfanos, aplica flags `HttpOnly` y `SameSite` en cookies de sesión. Documenta el cambio en el inventario técnico.

Para el analista · SOC, respuesta a incidentes

Lo que importa. Contexto de la amenaza en tiempo real — indicadores de compromiso, actividad observada en los componentes de la cadena, correlación con inteligencia de amenazas, señales de explotación activa en organizaciones pares del sector.

Lo que recibe de CSURFACE. Alertas correlacionadas con inteligencia de amenazas y con la postura externa del proveedor, indicación de explotación en curso, contexto temporal (cuándo apareció la señal, cuándo cambió, quién más fue afectado), enriquecimiento de IOCs para la investigación.

Cómo actúa. Investiga actividad anómala originada en componentes externos, conduce la contención cuando el vector es confirmado, comunica internamente, escala al ingeniero para corrección y al gestor para deliberación. Mantiene la traza forense.

APLICACIÓN Y RESULTADOS · PARTE 05

Previniendo el próximo Polyfill.io

Un caso de uso representativo y qué esperar en las primeras semanas de operación.

INVENTARIO TRADICIONAL

1×

proveedores conocidos y declarados en contrato — CDN, analytics, A/B, chat, AdTech.

→

TRAS EL MAPEO EN 3 NIVELES

49×

componentes en la cadena digital real — invisibles hasta que la cadena se despliega.

LO QUE CSURFACE OBSERVA · DATOS PROPIOS DE LA PLATAFORMA

2,8×
proveedores directos (Nivel 1) por cada activo propio en inventario

11×
expansión de la cadena sumando subproveedores (Nivel 2)

49×
tamaño real de la cadena desplegada hasta el Nivel 3

Escenario ilustrativo · e-commerce de mediano porte

Una operación de e-commerce con 12 sitios, tres frontends (web, web mobile y B2B) y más de 80 scripts JavaScript externos en el DOM activó el mapeo de CSURFACE. En la primera semana, la plataforma desplegó la cadena hasta el tercer nivel — **multiplicando en más de 40× el número de proveedores** que constaba en el inventario tradicional. Tres alertas críticas fueron emitidas:

CRÍTICO **Script de polyfill.io aún activo**
Un gestor de tags, en una página antigua, todavía apuntaba al dominio — nunca removido tras el incidente público.

ATENCIÓN **Dominio de CDN de chat expirando en 11 días**
Con riesgo de ser registrado por un tercero y pasar a servir código bajo el nombre de confianza.

CRÍTICO **Píxel de rastreo con nuevo dueño**
El proveedor cambió de propiedad dos meses antes — alteración de WHOIS detectada por la plataforma.

Time-to-value

- **Día 1** — onboarding; el crawl headless inicial se completa en pocas horas.
- **Día 3** — inventario completo de dependencias en los tres niveles.
- **Semana 1** — monitoreo continuo activo; primera alerta ante cada cambio.
- **Mes 1+** — operación continua, con panel de riesgo por proveedor.

¿Quiere descubrir el tamaño de su cadena digital — gratuitamente?

En un análisis preliminar sin costo, CSURFACE mapea los tres niveles de proveedores para uno de sus activos públicos y devuelve el informe técnico completo.

Mapear mi cadena →

CUMPLIMIENTO · PARTE 06

El mismo trabajo que protege y comprueba

Cómo el mapeo continuo de la cadena digital atiende requisitos regulatorios sin esfuerzo adicional.

Requisitos regulatorios atendidos

NORMA	REQUISITO	CÓMO CONTRIBUYE EL MAPEO
BACEN 4.557	Evaluación continua de proveedores críticos	**Monitoreo continuo, no puntual**
ISO 27001	Relación con proveedores (Anexo A)	**Inventario técnico verificable**
NIST CSF	Supply Chain Risk Management	**Mapeo en tres niveles**
PCI DSS 4.0	Gestión de proveedores de servicio (Req. 12.8)	**Lista de terceros siempre actual**
EU NIS2	Gestión de riesgo de cadena de suministro	**Evidencia de evaluación continua**

Aplicable a operaciones sujetas a cada regulación; la NIS2 rige para organizaciones con operación en la Unión Europea.

Cumplimiento como subproducto. El mapeo continuo de la cadena digital sirve, al mismo tiempo, a la seguridad y al cumplimiento. El inventario técnico, verificable y siempre actualizado es, al mismo tiempo, el control de seguridad y la evidencia que el auditor pide — sin retrabajo.

Del cuestionario a la evidencia técnica

El modelo tradicional comprueba el cumplimiento con un repositorio de cuestionarios autodeclarados. El mapeo de CSURFACE sustituye ese modelo por un inventario técnico continuamente actualizado:

- Cada proveedor identificado por inspección técnica directa.
- Cada cambio registrado con fecha y tipo de evento.
- Cada alerta crítica documentada de la detección a la resolución.

El resultado es una traza de auditoría que describe la cadena tal como existe técnicamente, establecida mediante inspección directa y verificable de los activos.

PRÓXIMOS PASOS

Descubra al subproveedor antes de que él lo descubra a usted

El análisis de la cadena digital de proveedores es una de las capacidades de la plataforma CSURFACE — una plataforma de Continuous Exposure Management. En una arquitectura integrada, reúne el descubrimiento continuo de la superficie externa con Machine Learning, el análisis de la cadena digital de proveedores, la validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie, la inteligencia de amenazas con priorización dinámica y el monitoreo de credenciales filtradas. Opera de forma íntegramente externa — sin agente y sin instalación —, con integraciones opcionales de nube, WAF y CIEM disponibles para organizaciones que buscan mayor profundidad de visibilidad.

Mapee uno de sus sitios

En una sesión técnica de 30 minutos, CSURFACE ejecuta el mapeo de la cadena digital de un activo de su elección en los tres niveles de profundidad.

Use la calculadora de riesgo

Estime la pérdida anual esperada de su sector con la calculadora de riesgo de CSURFACE, calibrada por benchmark de mercado.

Lea el whitepaper de ML Discovery

Descubrimiento continuo de la superficie externa con Machine Learning — la base sobre la cual opera el mapeo de proveedores.

Vea su cadena digital real — mapeada hasta tres niveles de profundidad

Recibir análisis preliminar gratuito