csurface

INFORME ANUAL · CYBER EXPOSURE

Estado de la Exposición Digital

Edición 2026 — Cómo crece la superficie de ataque, cómo se acelera la amenaza y por qué la distancia entre ambas es el verdadero riesgo. Datos agregados y anónimos de decenas de organizaciones.

ORGANIZACIONES EN LA BASE **68 + 16 detalladas**	ACTIVOS EXTERNOS MAPEADOS **122 mil**	PERÍODO **2026**
CLASIFICACIÓN **Público**	EDICIÓN **1ª — Anual**	FUENTE **Plataforma CSURFACE**

La lectura en tres partes

Lo que dicen los datos de este informe — y la única conclusión hacia la que convergen.

Edición 2026
CSURFACE

OPERAN EN 2+ NUBES

75%

superficie dispersa por múltiples proveedores

EXPLOIT PÚBLICO TRAS LA FALLA

5 días

tiempo medio hasta que existe código de ataque

VULNERABILIDAD DESDE HACE 5+ AÑOS

68%

de las organizaciones analizadas

Este informe reúne, de forma **agregada y anónima**, lo que CSURFACE observó al mapear la superficie de ataque externa de decenas de organizaciones — 68 con descubrimiento concluido en la plataforma y 16 sometidas a análisis detallado. Ninguna empresa es identificada.

Primero: la superficie crece sin gobierno. No es un inventario organizado — se dispersa por varias nubes, por entornos aprovisionados con prisa y rara vez apagados, por componentes de terceros incrustados en cada aplicación. Tres de cada cuatro organizaciones operan activos en dos o más nubes; la mitad, en tres o más. Y lo que entra casi nunca se mantiene: el 68% arrastra una vulnerabilidad abierta desde hace más de cinco años.

Segundo: la amenaza se acelera. Un exploit público funcional surge, en promedio, cinco días después de que se divulga una falla; la explotación activa, a los noventa. Las clases de falla más explotadas son, en su mayoría, fallas de aplicación web — exactamente la capa que el 71% de las aplicaciones analizadas deja sin WAF.

Tercero: el riesgo reside en la distancia entre las dos curvas. La defensa agrega y olvida activos en una escala de años. El atacante arma exploits en una escala de días. El incidente es la intersección previsible de esas dos velocidades sobre el mismo activo sin gobierno — un suceso de naturaleza estructural, estadísticamente esperado donde la defensa queda por detrás de la amenaza.

La conclusión de este informe. Ninguna de las dos curvas se resuelve de forma aislada. Descubrir todo sin priorizar sobrecarga al equipo; priorizar amenazas sin ver la superficie entera protege solo lo que ya era conocido. Reducir el riesgo exige **descubrimiento continuo de la superficie** e **inteligencia de amenazas** operando juntas, sin interrupción.

Base de datos

Organizaciones con descubrimiento concluido	**68**
Análisis detallados de superficie	**16**
Sectores representados	**11**
Activos externos mapeados	**122.095**
Vulnerabilidades analizadas	**2.361**
Amenazas emergentes monitoreadas	**2.954**

Sectores de los análisis detallados: automotriz, educación, gobierno, industria, logística, colegio profesional, previsión social, salud, servicios, tecnología y comercio minorista.

Todo el análisis es externo y pasivo. Datos anonimizados; ninguna organización es identificada.

PARTE 01

La superficie crece — y crece sin gobierno

De qué está hecha la superficie de ataque externa y por qué se expande más rápido que cualquier inventario.

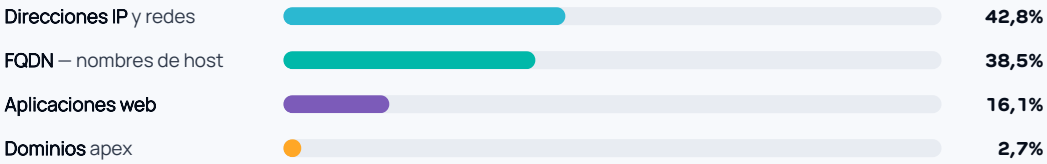
Edición 2026
CSURFACE

ACTIVOS EXTERNOS
122 mil
en 68 organizaciones

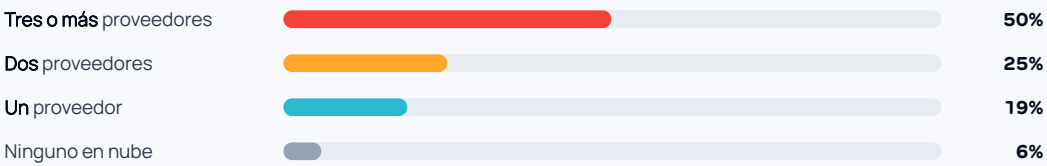
ORGANIZACIONES RELACIONADAS
1.068
descubiertas por la plataforma

COMPONENTES DE TERCEROS
2,8×
por activo propio expuesto

Distribución de los activos externos por tipo



Proveedores de nube por organización



Análisis

La superficie de ataque externa no es un inventario organizado. Se acumula. Cada equipo de producto publica una aplicación, cada área de negocio contrata un SaaS, cada adquisición trae la infraestructura heredada de otra empresa — y casi nada de eso se elimina después.

El dato más revelador es el de la nube: **tres de cada cuatro organizaciones** distribuyen activos por dos o más proveedores, y la mitad por tres o más. Cada entorno agrega una consola propia, un patrón de configuración propio y una frontera de gestión propia. Tratados en **silos aislados**, con herramientas, patrones y equipos distintos por proveedor, esos entornos generan vistas parciales que rara vez se reconcilian: la superficie real existe fragmentada entre múltiples consolas, y ninguna de las vistas parciales representa el todo.

La dependencia de terceros amplía el efecto: cada aplicación web expuesta arrastra múltiples componentes de la cadena de proveedores — scripts, CDN y bibliotecas incrustados en el código que expanden la superficie sin aparecer en ningún inventario.

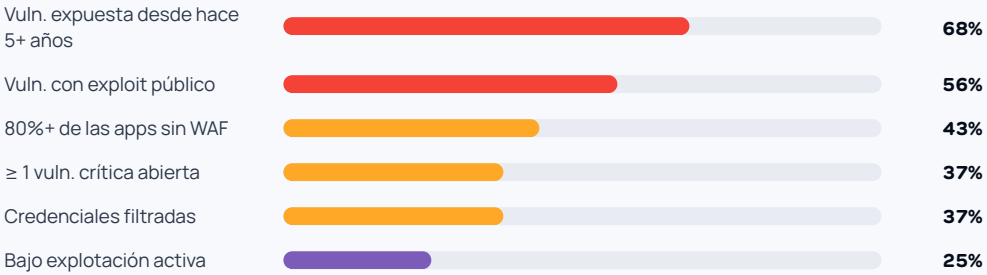
Por qué esto importa. El inventario es la base de todo programa de seguridad. Sin saber lo que existe, toda priorización, toda prueba y toda respuesta operan sobre una base incompleta — y lo que quedó fuera sigue expuesto.

PARTE 02

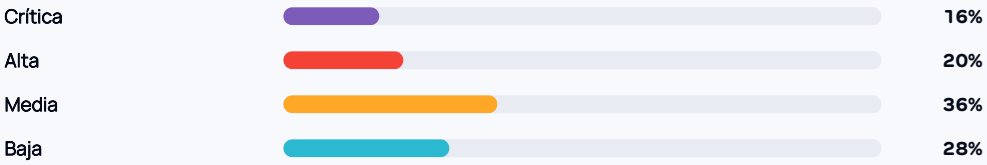
Lo que la superficie acumula

Los hallazgos que se repiten de empresa en empresa — y casi siempre son antiguos.

Frecuencia de los hallazgos — % de las empresas analizadas



Distribución de las 2.361 vulnerabilidades por severidad



La severidad no es prioridad

INDICADOR DE EXPLOTACIÓN	REPRESENTATIVIDAD
Con exploit público disponible	**5,7%** de las vulns
Comprobadamente explotadas	**1,8%** de las vulns
Conjunto realmente prioritario	**7,5%** de las vulns

De las 2.361 vulnerabilidades, solo una fracción tiene explotación comprobada — y es en esa fracción donde comienza un atacante.

El tiempo de exposición es el problema. En el 68% de las organizaciones hay una vulnerabilidad abierta desde hace más de cinco años; la más antigua registrada superaba una década. La edad media de las exposiciones supera los seis años. Se trata de un pasivo silencioso: vulnerabilidades antiguas que permanecieron fuera del radar de los inventarios y de los ciclos de corrección. El backlog de remediación, medido en años, es incompatible con la velocidad de la amenaza.

Análisis

Los mismos hallazgos se repiten de empresa en empresa, y casi siempre son **antiguos**. La superficie crece y acumula. Lo que entra rara vez se elimina; lo que falla rara vez se corrige.

El volumen de vulnerabilidades engaña. Lo que separa un inventario de riesgo de una lista interminable es la inteligencia de explotación: saber qué fallas tienen exploit, cuáles se están usando, cuáles tienen probabilidad real de ataque. Sin ese filtro, el equipo atiende lo que es ruidoso — no lo que es peligroso.

PARTE 03

Del otro lado, la amenaza no espera

El ritmo de la explotación observado en el recorte de mayor riesgo — fracción de aproximadamente 1% de las vulnerabilidades, seleccionada por threat intelligence, exploit intelligence y Machine Learning.

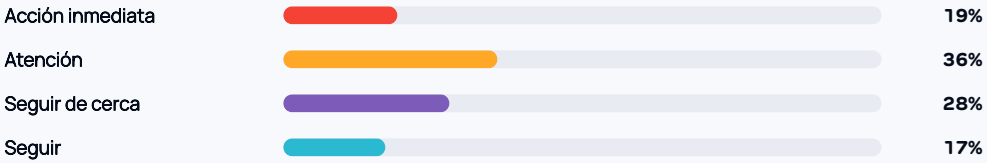
Edición 2026
CSURFACE

Sobre el recorte. La plataforma de CSURFACE detecta el universo completo de vulnerabilidades en cada activo monitoreado. Los números de esta parte se refieren a la fracción de aproximadamente **1% con mayor potencial de generar un incidente** — identificada por el cruce de **threat intelligence**, **exploit intelligence** y **Machine Learning** sobre esa base. Es sobre ese recorte priorizado que se mide el ritmo de la explotación en el mundo real.

AMENAZAS EMERGENTES MONITOREADAS	EXPLOIT PÚBLICO EN	EXPLOTACIÓN ACTIVA EN	EN EXPLOTACIÓN REAL
2.954	**5 días**	**90 días**	**809**
recorte priorizado · alta severidad	tiempo medio tras la divulgación	tiempo medio hasta ataque en el mundo real	confirmadas explotadas en el mundo

Clases de falla más explotadas (CWE)

Prioridad real — categorización SSVC



Análisis

Mientras la superficie se acumula en silencio, la amenaza del otro lado se mueve a **ritmo industrial**. Un exploit público funcional surge, en promedio, cinco días después de la divulgación de una falla. En parte de los casos el exploit llega antes del aviso: entre las amenazas críticas monitoreadas hay cientos explotadas como zero-day.

La puntería del atacante es precisa. Cinco de las seis clases de falla más explotadas son fallas de **aplicación web** — inyección, path traversal, carga de archivo. Es exactamente la capa que, en la Parte 02, aparece sin WAF en el 71% de las aplicaciones analizadas. La curva de la amenaza apunta al punto más desprotegido de la defensa.

Y la severidad no es prioridad: incluso en un conjunto donde toda falla es grave — CVSS medio 9,0 — la categorización SSVC clasifica solo **el 19% como acción inmediata**. Leer indicadores de explotación lo logra cualquier equipo; lo difícil es cruzar esa inteligencia con la superficie real y saber, cada semana, qué amenazas alcanzan los propios activos.

La lista no para de crecer. El catálogo de vulnerabilidades comprobadamente explotadas se actualiza cada semana — una sola semana reciente registró 12 nuevas entradas. Un escaneo trimestral pierde la ventana entera. Solo el monitoreo continuo detecta la falla en la semana en que se convierte en una amenaza confirmada.

LA CONCLUSIÓN

El encuentro — donde el incidente nace

Qué tiene que ver el volumen de amenazas con los informes de superficie.

Edición 2026
CSURFACE

LA AMENAZA ATACA

5 días

tiempo medio entre que una falla se divulga y existe un exploit público funcional para ella.

×

LA PUERTA QUEDA ABIERTA

5+ años

tiempo que la vulnerabilidad más antigua permanece expuesta en el 68% de las empresas analizadas.

El análisis

Todo. Esa es la respuesta a qué tiene que ver el volumen de amenazas con los informes de superficie. Cada activo sin gobierno de la Parte 01 — un entorno en nube olvidado, un componente de terceros, una aplicación sin WAF — es una puerta. La Parte 03 dice que las puertas se encuentran y se atacan en días. Los informes de la Parte 02 dicen que esas puertas quedan abiertas durante años.

Lado a lado, los dos conjuntos de datos convergen en una sola conclusión. La defensa agrega activos más rápido de lo que consigue inventariarlos, y elimina o corrige casi nada — el tiempo de exposición se mide en **años**. El atacante arma un exploit en **días**.

Un incidente, por tanto, es la intersección previsible de dos curvas: una superficie que crece desordenada y nunca se reduce, y una amenaza que solo se acelera. El incidente es apenas la vez en que ambas se cruzan sobre el mismo activo — casi siempre un activo ausente del inventario.

Lo que cierra la distancia entre las dos curvas

No se corrige una superficie que no se ve, ni se vence la velocidad de la amenaza con esfuerzo manual. Cerrar esa distancia exige dos capacidades operando juntas y sin parar:

Descubrimiento continuo — que encuentra cada puerta, incluidos los entornos en nube, el shadow IT y los activos ausentes del inventario.

Inteligencia de amenazas y exploits — que dice qué puertas están siendo atacadas ahora, y reordena la fila de prioridad conforme la amenaza evoluciona.

Una sin la otra deja la ventana abierta. Es la combinación continua de ambas — descubrimiento e inteligencia en el mismo modelo de datos — la que transforma la exposición en riesgo gestionable.

csurface

CONTINUOUS EXPOSURE MANAGEMENT

De la exposición desordenada a la acción priorizada.

CSURFACE es una plataforma única de gestión de superficie de ataque externa. Reúne, bajo un solo modelo de datos, las dos capacidades que este informe muestra ser inseparables: descubrir todo lo que está expuesto y saber, en tiempo real, lo que la amenaza va a explotar primero.

Descubrimiento continuo

Mapea toda la superficie externa a partir del dominio raíz — nube, shadow IT, cadena de terceros y activos olvidados. Sin agentes, sin listas que proporcionar.

Clasificación por Machine Learning

Atribuye cada activo a la organización, elimina el falso positivo de propiedad y clasifica por criticidad de negocio. Un inventario con contexto.

Inteligencia de amenazas y exploits

Cruza cada exposición con índices de explotación activa y amenazas emergentes — la fila de prioridad refleja el riesgo real y se reordena sola.

Validación de explotabilidad

Confirma lo que es de hecho explotable, con prueba activa externa donde hay cobertura y detección pasiva en el resto de la superficie.

Monitoreo de credenciales

Da seguimiento a las credenciales corporativas filtradas en brechas y en la dark web, con alerta en horas — no en meses.

Cuantificación de riesgo

Capacidad en desarrollo: traducirá el riesgo técnico en valor financiero, para que la dirección decida con base en números, no en alertas técnicas.

Vea dónde está su empresa en este retrato.

Recibir el análisis preliminar de mi empresa →