CSURFACE

WHITEPAPER · THREAT INTELLIGENCE

Priorización de vulnerabilidades más allá del CVSS

Threat Intelligence y priorización dinámica: cómo acertar la cola de remediación combinando severidad técnica, explotabilidad real (índice de probabilidad de explotación y catálogo de explotación activa) y criticidad del activo.

CAPACIDAD	PÚBLICO	EDICIÓN
Threat Intelligence	CISO · Vuln. Manager · SOC	2026

LECTURA	CLASIFICACIÓN	FUENTE
9 páginas	Público	Plataforma CSURFACE

RESUMEN EJECUTIVO

La cola correcta de remediación es dinámica

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

CVES DETRÁS DE LAS BRECHAS

5%

de las CVEs responden por el 20% de las violaciones reales

VENTANA DE ARMAMENTIZACIÓN

24h

el 28% de las vulnerabilidades explotadas se arman en 24 horas

REMEDIACIÓN MENSUAL TÍPICA

15%

del backlog se corrige por mes — insuficiente para contener el ritmo de ingreso

La mayoría de los programas de Vulnerability Management prioriza por el CVSS. Es una elección intuitiva y técnicamente insuficiente. El CVSS cuantifica la **severidad técnica teórica** de una vulnerabilidad — el impacto que produciría *si* fuera explotada. No indica si **está siendo explotada en el presente**, ni pondera la criticidad del activo en el que reside.

El resultado es una cola sistemáticamente desalineada con el riesgo real. Los equipos asignan capacidad escasa a vulnerabilidades de CVSS elevado y baja explotabilidad, mientras vulnerabilidades de severidad media — pero activamente explotadas en campañas en curso — permanecen abiertas. Apenas **el 5% de las CVEs responden por el 20% de las violaciones** (Verizon DBIR 2024); priorizar por el CVSS es, en la práctica, ignorar esa concentración de riesgo.

Este whitepaper presenta el enfoque de CSURFACE: **priorización dinámica en tres ejes** — severidad técnica, explotabilidad real (vía índice de probabilidad de explotación y catálogo de explotación activa) y criticidad del activo —, reevaluada continuamente conforme el escenario de amenazas evoluciona. Una CVE de 7.5 puede convertirse en prioridad máxima al día siguiente de su ingreso al catálogo de explotación activa. La cola debe reflejar esa dinámica.

La tesis. La priorización eficaz es un problema de inteligencia de amenazas. La cola adecuada constituye un ranking dinámico, reordenado cada vez que un exploit se vuelve disponible, una familia de ransomware incorpora la vulnerabilidad o los catálogos de explotación activa la confirman. Las listas fijadas en el momento del *disclosure* quedan desalineadas en días.

Qué cubre este whitepaper

- Por qué el volumen de CVEs creció — y por qué el CVSS no escala con él.
- Las tres razones por las cuales el CVSS, solo, lleva a la cola equivocada.
- El modelo de priorización en tres ejes de CSURFACE.
- Cómo el feed de inteligencia se mantiene dinámico y un caso de uso real.

EL ESCENARIO · PARTE 01

El crecimiento de vulnerabilidades — y la cola que no retrocede

Volumen de publicaciones, capacidad de remediación y la razón por la cual la pregunta central dejó de ser cuantitativa.

~30 mil
CVEs publicadas en 2024 — 15% más que en 2023; 2025 se aproximó a 48 mil

~15 mil
vulnerabilidades por año en el inventario de una organización de porte medio

15% / mes
tasa típica de remediación del backlog — por debajo del ritmo de ingreso de nuevas CVEs

El volumen creció más rápido que la capacidad

El número de CVEs publicadas cada año dejó de ser un detalle administrativo y se convirtió en un problema de capacidad. Fueron cerca de **30 mil CVEs en 2024** — 15% más que en 2023 — y 2025 se aproximó a **48 mil**, un salto del orden del 60%.

Una organización de porte medio debe lidiar con algo cercano a **15 mil vulnerabilidades por año** en su inventario. La tasa típica de remediación, sin embargo, queda alrededor del **15% del backlog por mes** (Cyentia). El diferencial entre ingreso y salida es negativo de forma estructural: el backlog crece consistentemente.

Ante esa asimetría, la pregunta central deja de ser *"¿cuántas vulnerabilidades tenemos?"* y pasa a ser: **"¿estamos corrigiendo las que representan riesgo real?"**

Estadísticas clave

Violaciones concentradas en pocas CVEs	5%→20%
Explotadas y armadas en hasta 24h del disclosure	28%
Remediación mensual típica del backlog	15%
Tiempo medio entre disclosure y patch	20 días

Fuentes: Verizon DBIR 2024, CISA 2024, Cyentia, Snyk — informes públicos.

El costo de errar la cola. El costo medio de una violación de datos en Brasil llegó a **€3,90M** en 2025 (IBM Cost of a Data Breach 2025). Cada vulnerabilidad activamente explotada postergada en la cola representa exposición directa por el período del atraso. Priorizar con precisión representa la distinción entre un programa de remediación que efectivamente reduce riesgo y uno que absorbe capacidad sin dirigir el esfuerzo al punto de mayor probabilidad de impacto.

Por qué esto importa. La capacidad de remediación es finita y no acompañará el volumen de CVEs. La única palanca real es el orden de la cola: corregir primero lo que tiene mayor probabilidad de ser explotado, en el activo que más importa.

POR QUÉ EL CVSS FALLA · PARTE 02

El CVSS mide impacto teórico — no riesgo real

Las tres razones por las cuales priorizar exclusivamente por la puntuación CVSS lleva al objetivo equivocado.

Whitepaper 2026
CSURFACE

POR EL CVSS · CORRIGE PRIMERO

9.8

CVSS "crítica" — pero sin exploit público, ausente de kits de ransomware y exigiendo condiciones rarísimas de entorno para funcionar.

→

POR LA REALIDAD · ES LA URGENCIA

7.5

CVSS "alta" — con exploit público publicado, en el catálogo de explotación activa y activamente usada por familias de ransomware en campañas reales.

Un número, tres puntos ciegos

El CVSS cuantifica el impacto teórico *en caso de que* la vulnerabilidad sea explotada. No responde a la pregunta operativa — ¿**está siendo explotada ahora?**. El contraste anterior resume el problema: por el CVSS, el equipo corrige la 9.8 primero; por la realidad del riesgo, la 7.5 es la urgencia. La puntuación técnica, sola, conduce a la decisión inversa a la correcta.

El motivo es estructural. Las tres razones a continuación explican por qué priorizar exclusivamente por la puntuación CVSS lleva al objetivo equivocado — y por qué ninguna de ellas se resuelve calibrando mejor el propio CVSS.

Razón 01 · el CVSS mide severidad, no explotabilidad. La puntuación responde "cuán grave sería", no "esto está siendo explotado". Es el eje que el ejemplo anterior expone.

Razón 02 · el CVSS ignora el contexto del activo. Una vulnerabilidad 9.8 en un servidor de producción con datos de tarjeta es catastrófica. La misma 9.8 en una máquina de prueba aislada, sin datos, es prácticamente irrelevante. El CVSS atribuye a ambas el mismo número — y cualquier cola construida solo sobre él trata casos incomparables como iguales.

LO QUE CSURFACE OBSERVA · DATOS PROPIOS DE LA PLATAFORMA

5,7%
de las 2.361 vulnerabilidades analizadas tienen exploit público — y solo el 1,8% están en el catálogo de explotación activa

19%
de un feed de amenazas de CVSS medio 9,0 exigen acción inmediata en la categorización SSVC

~5 días
es el tiempo medio hasta que surge un exploit público tras la divulgación de una falla

Razón 03. El CVSS es estático; el riesgo cambia continuamente

La puntuación se atribuye en el *disclosure* y raramente se revisa. El escenario de amenazas, sin embargo, evoluciona en días. Observe la trayectoria típica de una misma CVE:

1. **Día 0 — disclosure.** La CVE recibe CVSS 7.5. La cola la coloca como prioridad media.
2. **Día 3 — prueba de concepto.** Un exploit funcional se publica en un repositorio público. La barrera para el ataque se desploma.
3. **Día 7 — adopción criminal.** Las familias de ransomware pasan a incorporar la vulnerabilidad a sus campañas.
4. **Día 14 — confirmación oficial.** La CVE entra en el catálogo de explotación activa, atestiguando explotación activa en ataques reales.

El CVSS continúa 7.5 del día 0 al día 14. El riesgo real, en ese intervalo, subió varias veces — y la cola estática nunca registró el cambio.

EL ENFOQUE CSURFACE · PARTE 03

Priorización dinámica en tres ejes

Severidad técnica, explotabilidad real y criticidad del activo — combinadas en un único score vivo.

LOS TRES EJES DE LA PRIORIZACIÓN DINÁMICA

1

Severidad técnica

El CVSS como *baseline* de impacto, en escala de 0 a 10. Eje estable — raramente cambia tras el disclosure.

2

Explotabilidad real

La probabilidad concreta de explotación, informada por índice de probabilidad de explotación, catálogo de explotación activa, inteligencia activa y ransomware.

3

Criticidad del activo

El peso del activo ajusta la posición de la misma vulnerabilidad según dónde aparece en la organización.

Qué compone la explotabilidad real

El Eje 02 es lo que el CVSS no cubre. Reúne evidencias independientes de explotación, cada una con su propia cadencia de actualización:

CRÍTICO **Probabilidad de explotación**
Estima la probabilidad estadística de explotación en los próximos 30 días, actualizada diariamente.

CRÍTICO **Catálogo de explotación activa**
Catálogo de vulnerabilidades comprobadamente explotadas en ataques reales. Constar en él significa prioridad automática.

ATENCIÓN **Inteligencia activa**
Monitoreo de kits de explotación, foros de comercio criminal y repositorios públicos de pruebas de concepto.

ATENCIÓN **Indicadores de ransomware**
Asociación a familias activas — señal de adopción operativa de la vulnerabilidad por atacantes.

El score final

Los tres ejes se combinan en una única lectura de prioridad, reevaluada continuamente:

> La plataforma prioriza por la explotación activa observada y por la criticidad del activo, combinando severidad técnica e inteligencia de amenazas — de forma auditable, sin exigir que el cliente conozca la mecánica interna de ponderación.

Una explotación activa observada en un activo crítico asume la cima; una severidad alta sin señal de explotación retrocede en la cola.

Cómo se clasifica el activo. CSURFACE evalúa sensibilidad de datos (personales y sensibles bajo RGPD, datos de tarjeta bajo PCI), exposición (público, intranet o segregado), criticidad de negocio y posición en la cadena — de frontend orientado al cliente a backoffice.

Por qué pesa la explotación. Una severidad elevada sin explotación observada retrocede en la cola, mientras que la explotación activa en un activo crítico asume la cima. La cola refleja el riesgo vigente, y no solo el impacto teórico de la vulnerabilidad.

EL ENFOQUE CSURFACE · PARTE 03

Un feed de inteligencia continuamente actualizado

Las fuentes integradas y el ciclo cerrado que reordena la cola de prioridades sin dependencia de intervención manual.

Whitepaper 2026
CSURFACE

EL CICLO CERRADO DE REEVALUACIÓN — SIN INTERVENCIÓN MANUAL

1. **Reevaluación automática**
   El score de prioridad se recalcula sin ningún accionamiento manual cuando la CVE cambia de estado.
2. **Notificación dirigida**
   Cambios materiales — como la entrada de una CVE en el catálogo de explotación activa — generan alerta inmediata.
3. **Ticket sincronizado**
   El ticket en Jira o ServiceNow se actualiza, y el SLA acompaña la nueva prioridad.
4. **Panel ejecutivo actualizado**
   El panel de gestión refleja la cola reordenada en tiempo real, prescindiendo del ciclo periódico de informe.

Fuentes integradas

La priorización solo es dinámica porque el feed de inteligencia también lo es. CSURFACE integra y cruza, de forma continua:

- CRÍTICO **Probabilidad de explotación**
  Feed diario de probabilidad de explotación.
- CRÍTICO **Catálogo de explotación activa**
  Catálogo de explotación activa, actualizado en horas.
- **NVD**
  Datos base de las CVEs y sus metadatos oficiales.
- **Avisos de fabricantes**
  Boletines de seguridad de los proveedores afectados.
- ATENCIÓN **Pruebas de concepto públicas**
  Incluyendo Exploit-DB y repositorios abiertos.
- ATENCIÓN **Monitoreo criminal**
  Discusión y comercio de exploits en foros cerrados.
- ATENCIÓN **Señales de honeypot**
  Cuando una vulnerabilidad comienza a ser escaneada a gran escala.

Por qué el feed debe ser continuo

Una cola estática solo sería suficiente si el escenario de amenazas también lo fuera. Un exploit puede surgir tres días después del disclosure; los catálogos de explotación activa pueden confirmar la explotación pocos días después. Cada uno de esos cambios altera la prioridad real de una CVE — y, si el feed no los registra el mismo día, la cola opera sobre datos desactualizados, desconectada del riesgo vigente.

Por eso CSURFACE trata la inteligencia como un flujo continuo. Cada fuente al lado tiene cadencia propia, y el ciclo cerrado descrito arriba garantiza que todo cambio material alcance la cola — y al equipo responsable — sin depender de la percepción individual de un analista.

Ritmo de cada eje. La severidad técnica es prácticamente estática. La explotabilidad se reevalúa diariamente — el índice de probabilidad de explotación corre todos los días, el catálogo de explotación activa en horas, la inteligencia activa en tiempo real. La criticidad del activo se revisa mensualmente o con cada cambio de configuración.

APLICACIÓN Y RESULTADOS · PARTE 04

El mismo equipo, una cola diferente

Un caso de uso representativo: cómo la priorización dinámica reordenó la cima de la cola sin aumentar la capacidad.

PRIORIZACIÓN POR CVSS

3

incidentes materiales en 12 meses — todos en CVEs de CVSS 7.x, pero presentes en el catálogo de explotación activa.

→

PRIORIZACIÓN DINÁMICA CSURFACE

0

incidentes materiales en los 6 meses siguientes, con el mismo equipo y la misma capacidad de remediación.

Caso de uso · banco de porte medio

Una institución financiera de porte medio operaba con **4.200 activos** y cerca de **8.700 CVEs activas**. El equipo — cuatro responsables de corrección y dos desarrolladores — tenía capacidad para cerca de 80 correcciones por mes, contra un backlog que crecía 50 por mes. La cola priorizaba las 200 vulnerabilidades de CVSS 9.0 o más.

Los tres incidentes registrados en doce meses ocurrieron, todos, en vulnerabilidades de CVSS en la franja 7.x — por debajo del corte de "crítica" — pero presentes en el catálogo de explotación activa. La cola por CVSS las había dejado fuera.

Con la priorización dinámica, la cima de la cola fue reordenada sin alterar la capacidad del equipo.

Cómo cambió la cima de la cola

47 vulnerabilidades salieron de la lista de críticas
CVSS alto, pero con probabilidad de explotación muy baja y sin ninguna señal de explotación.

CRÍTICO **89 entraron en la cima de la cola**
CVSS medio, pero con probabilidad de explotación elevada o ya en el catálogo de explotación activa.

ATENCIÓN **31 subieron de posición**
Exclusivamente por la criticidad del activo.

El resultado. La capacidad de remediación pasó a dirigirse hacia donde el riesgo efectivamente estaba concentrado. En los seis meses siguientes, los incidentes materiales cayeron de tres a cero — sin ampliación de equipo ni presupuesto adicional.

La capacidad no cambió — la asignación sí. El equipo mantuvo el ritmo de cerca de 80 correcciones por mes. Lo que se alteró fue la composición de esas correcciones: el esfuerzo dejó de ser absorbido por vulnerabilidades de CVSS elevado sin explotación activa y pasó a cubrir las que presentaban explotación real en los activos de mayor criticidad.

APLICACIÓN Y RESULTADOS · PARTE 04

Métricas de cambio e integración en la plataforma

Variaciones en los indicadores del programa y articulación de la priorización dinámica con las demás capacidades de la plataforma.

Métricas de cambio · banco de porte medio

INDICADOR	ANTES · PRIORIZACIÓN POR CVSS	DESPUÉS · PRIORIZACIÓN DINÁMICA	VARIACIÓN
MTTR de vulnerabilidades críticas explotadas	87 días	**18 días**	-79%
Correcciones aplicadas en CVEs con explotación real	45%	**92%**	+47 pp
Saldo mensual del backlog	+50	**-12**	revertido
Falsos positivos en la cola crítica	Alto	**Bajo**	Reducción material
Incidentes materiales por año	3	**0** (en 6 meses)	-100%

Indicadores observados en el caso de uso descrito en la página anterior. Los resultados varían según el tamaño del inventario, la capacidad de remediación y la madurez del programa de cada organización.

-79%
en el MTTR de las vulnerabilidades críticas explotadas — de 87 a 18 días

backlog
saldo mensual revertido: de +50 vulnerabilidades por mes a -12

3 → 0
incidentes materiales — de tres en doce meses a cero en los seis meses siguientes

Integración con las demás capacidades

La Threat Intelligence no opera de forma aislada. En la plataforma unificada de CSURFACE, consume las demás capacidades y retroalimenta cada una de ellas:

Descubrimiento continuo
Cada nuevo activo de la superficie externa entra automáticamente en el alcance de la priorización.

Validación de explotabilidad
Validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie.

CRÍTICO **Monitoreo de credenciales filtradas**
Credenciales comprometidas sumadas a una vulnerabilidad crítica elevan la prioridad al máximo.

De la cola al valor financiero. La prioridad calculada alimenta la calculadora de riesgo de CSURFACE, que estima la pérdida anual esperada por sector. Cuanto mayor la prioridad de una vulnerabilidad, mayor el costo de mantenerla abierta — una lectura que traduce la cola técnica a lenguaje de negocio accesible al consejo y al comité de auditoría.

Indicadores clave del programa

- MTTR de las vulnerabilidades efectivamente explotadas — no del promedio general del backlog.
- Porcentaje del esfuerzo de remediación aplicado a CVEs con explotación confirmada.
- Saldo neto mensual del backlog: tendencia de reducción o crecimiento.

PRÓXIMOS PASOS

La cola correcta comienza con inteligencia de amenazas

La Threat Intelligence con priorización dinámica es una de las capacidades de la plataforma CSURFACE — una plataforma de Continuous Exposure Management. En arquitectura unificada, reúne descubrimiento continuo de la superficie externa con Machine Learning, análisis de la cadena digital de proveedores, validación de explotabilidad, inteligencia de amenazas con priorización dinámica y monitoreo de credenciales filtradas. Opera integralmente de forma externa — sin agente y sin instalación —, con integraciones opcionales de nube, WAF y CIEM para organizaciones que demandan visibilidad profunda de entornos internos.

Evalúe cómo se reordenaría su cola

En una demostración de 30 minutos, presentamos cómo la lista de prioridades actual se reorganizaría con la priorización dinámica en tres ejes.

Calculadora de riesgo financiero

Estime la pérdida anual esperada por sector y cuantifique el costo de mantener cada vulnerabilidad abierta.

Whitepaper: ML Discovery

Descubrimiento continuo de la superficie externa — la base de inventario sobre la cual toda priorización dinámica debe operar.

Conozca su cola reordenada — por la explotación real, no por la puntuación teórica

Solicitar análisis preliminar