CLOUDFLARE

2026

Informe de seguridad Cloudflare Signals

Resiliencia autónoma

PRÓLOGO DE MICHELLE ZATLYN

Todo está cambiando.

La IA avanza de la fase piloto a la producción, los sistemas autónomos aceleran la toma de decisiones y la economía digital evoluciona en tiempo real. Para los líderes dispuestos a actuar, este ritmo de cambio ofrece una oportunidad real.

La resiliencia se ha convertido en la nueva ventaja competitiva. Los sistemas inteligentes redefinen la economía digital, y los líderes pueden diseñar medidas de protección para anticiparse a los cambios, desarrollar sistemas que se adapten a ellos y convertir la volatilidad en una ventaja.

Cloudflare opera una de las redes globales más grandes del mundo, que abarca más de 330 ciudades en más de 120 países. Protegemos millones de propiedades de Internet, evitamos más de 230 000 millones de ciberataques al día y gestionamos 2500 millones de solicitudes de bots cada día. Esta posición estratégica nos permite observar tanto los riesgos como las oportunidades que modelan Internet.

El informe de seguridad Cloudflare Signals 2026 ofrece la información útil que necesitan los líderes hoy en día, identificando las fuerzas que redefinen el panorama digital, para que puedas controlar los sistemas inteligentes, proteger la modernización y desarrollar la resiliencia desde la base.

Nuestra misión es ayudar a mejorar Internet. En 2026, eso significa ayudarte a proteger tus operaciones, con total confianza y a la velocidad de las máquinas.

Michelle Zatlyn
Cofundadora, presidenta
y copresidenta de Cloudflare

RESUMEN EJECUTIVO

Para las empresas muy interconectadas y automatizadas actuales, el modelo de "amortiguar el impacto y garantizar la recuperación" ya no funciona.

Este enfoque se basa en la hipótesis ingenua según la cual podemos prever con precisión cada interrupción específica y prepararnos adecuadamente para cada una de ellas. Los sistemas de IA actúan de forma autónoma. Las plataformas en la nube concentran las cargas de trabajo críticas. Las cadenas de suministro se adentran en ecosistemas opacos. En esta nueva realidad, los responsables de la seguridad necesitan una **resiliencia autónoma: sistemas que no solo resistan las situaciones difíciles, sino que apliquen normativas, se adapten y se recuperen en tiempo real**.

Sin embargo, aunque muchas organizaciones parecen maduras, modernas y bien administradas, la resiliencia autónoma no es perceptible en una situación de estabilidad. Es una calidad de liderazgo que solo se revela en situaciones difíciles y continuadas.

Este informe parte de una premisa básica: los mayores riesgos que afrontarán las empresas en 2026 no están relacionados con las vulnerabilidades evidentes. Surgen de desafíos ocultos, es decir, de áreas que parecen adecuadas cuando todo funciona con normalidad, pero que pueden fallar fácilmente cuando las operaciones empresariales se aceleran, se amplían o afrontan interrupciones.

En estos capítulos, proporcionamos a los ejecutivos un plan para identificar estos desafíos antes de que causen interrupciones. Cada sección plantea preguntas específicas para suscitar el debate interno e identificar los puntos débiles ocultos en las propias empresas. En la era de la información, la autonomía y la velocidad, el éxito corresponde a los líderes que diseñan estructuras empresariales que pueden detectar, adaptarse y autocorregirse en las situaciones difíciles, al mismo tiempo que protegen los resultados críticos ante las situaciones cambiantes.

Seis desafíos críticos

Estos desafíos no son independientes. La presión en un área puede intensificar la vulnerabilidad en otras.

1 Dominar el algoritmo: controlar la IA a gran escala

Los programas de IA suelen dar la impresión de ser rigurosos y estar adecuadamente gobernados y guiados por valores. Sin embargo, cuando se analizan más de cerca, muchos líderes no pueden explicar claramente dónde se ejecuta la IA, los datos a los que tiene acceso ni quién es el responsable en caso de fallo. El progreso superficial a menudo oculta deficiencias en materia de visibilidad y propiedad que quedan expuestas cuando los reguladores, los clientes o los incidentes ejercen presión.

2 La confianza a la velocidad de las máquinas: desarrollar para la autonomía

Los sistemas autónomos funcionan bien cuando las condiciones son predecibles. En situaciones difíciles, la toma de decisiones es más rápida de lo que permite la supervisión humana, y la confianza se supone, en lugar de ser una característica integrada en el sistema. Este desafío permite evaluar si la delegación ha sido deliberada o si la autoridad se ha transferido discretamente a las máquinas sin límites ni una responsabilidad claramente definidos o sin un control en tiempo real.

3 Cadenas de suministro en la sombra: exponer las dependencias ocultas

Las empresas parecen diversificadas y tener numerosos socios, pero en realidad dependen de capas de servicios de terceros (y de los proveedores de estos) sobre los que no tienen una visibilidad integral. Cuando se produce una interrupción, el primer fallo no suele ser la respuesta, sino la detección. Este desafío revela si el riesgo de dependencia es intencional y visible, o heredado y opaco.

4 Señales de intención: de la información a la previsión

Aunque los programas de información basados en datos suelen parecer exhaustivos, los conocimientos recibidos demasiado tarde no influyen en las decisiones. Esta desafío distingue a las organizaciones que utilizan señales tempranas para perfeccionar continuamente sus decisiones, reforzar su previsión y mejorar su capacidad de respuesta a lo largo del tiempo, de aquellas que aprenden solo después de que el daño ya esté hecho.

5 La trampa de la deuda: la arquitectura heredada como riesgo estratégico

Las arquitecturas heredadas pueden parecer estables en las operaciones cotidianas. Sin embargo, ante los rápidos ataques modernos y el escrutinio normativo, resultan frágiles y consumen tiempo, talento y resiliencia a una velocidad que supera la capacidad de adaptación de las organizaciones. Este desafío expone si la arquitectura facilita la evolución o si por el contrario la limita.

6 Espejismo en la nube: desvinculación del riesgo en cascada

Las estrategias de nube prometen escala y eficiencia, pero los planos de control compartidos y las estrechas dependencias concentran los puntos de fallo. Ante situaciones difíciles, todo el sistema se derrumba. Esto permite verificar si la resiliencia está diseñada para la contención o si simplemente se asume por la existencia de planes de recuperación. Las organizaciones maduras limitan el alcance de los incidentes y mejoran su tolerancia a los fallos con cada interrupción.

Contenido

1

Dominar el algoritmo: controlar la IA a gran escala

Dominar el algoritmo: controlar la IA a gran escala

La adopción de la IA se acelera a un ritmo que supera la capacidad de adaptación de los modelos de gobernanza empresarial. Lo que comenzó como una experimentación aislada se ha integrado en los flujos de trabajo, las herramientas para desarrolladores, las interacciones con los clientes y el software de terceros que las organizaciones consumen pero que no controlan directamente. Sin embargo, antes de que la IA pueda actuar de forma independiente, es necesario haber implementado ya la visibilidad, la propiedad y las restricciones. Una vez que las decisiones se mueven a la velocidad de las máquinas, estas cuestiones ya no podrán debatirse.

Si bien la mayoría de los equipos ejecutivos reconocen que la IA es un problema de los consejos de administración, pocos pueden explicar claramente dónde se utiliza la IA, los datos que utiliza o cómo se gestiona el riesgo en toda su empresa. Esta brecha entre la sensibilidación sobre la IA y el control de la IA es ahora uno de los puntos ciegos más importantes para los equipos directivos de las empresas modernas.

La pregunta ya no es si la IA aporta valor. Se trata de si el equipo directivo tiene una visibilidad suficiente para controlar el impacto de la IA en la resiliencia, la confianza, el coste y la responsabilidad a gran escala.

La IA ya no es experimental. Opera en el corazón de la empresa, y debe regularse con el mismo rigor que las cuestiones financieras, de riesgo y normativas. En este entorno, la confianza es el verdadero factor diferenciador.

La velocidad gana. El permiso pierde.

La accesibilidad de la IA ha cambiado radicalmente la forma en que la tecnología entra en la organización. Los empleados y los equipos ya no esperan la aprobación centralizada. Las herramientas de IA se adoptan discretamente (a través de extensiones del navegador, funciones SaaS integradas, API y plataformas para desarrolladores), a menudo con buenas intenciones y ventajas inmediatas en términos de productividad.

La consecuencia es predecible: la IA se propaga más rápido que su gobernanza. De hecho, el 98 % de los empleados utilizan aplicaciones no autorizadas en numerosos casos de uso de Shadow AI y Shadow IT.[1]

Las herramientas no autorizadas introducen controles de seguridad incoherentes y prácticas de gestión de datos poco claras, y difuminan la responsabilidad. Para los consejos de administración, esto crea una realidad delicada. Los riesgos relacionados con la IA son importantes, pero a menudo apenas están cuantificados y no se tienen en cuenta.

Esto no refleja una falta de disciplina. Se trata de un desajuste estructural entre los modelos de aprobación heredados y la curva de adopción fluida de la IA.

La gobernanza ya no puede ser un paso de aprobación. Debe ser un sistema siempre activo basado en medidas de protección, una visibilidad continua y normativas que puedan evolucionar al ritmo de la adopción de la IA.

Los datos son un premio y una responsabilidad.

El valor de los sistemas de IA depende del acceso: a los datos, a los modelos y a las decisiones posteriores. Ante la presión de los resultados rápidos, las organizaciones suelen ampliar el acceso más rápido de lo que refuerzan los controles. Los límites de los derechos se difuminan. Los flujos de datos se vuelven opacos. Los servicios menos fiables se acercan a la información confidencial. El 97 % de las organizaciones que informaron de un incidente de seguridad relacionado con la IA en 2025 carecían de controles de acceso adecuados para la IA.[2]

Los marcos de seguridad tradicionales no se diseñaron para identificar los riesgos nativos de la IA, como la manipulación de instrucciones, la retención no intencionada de datos o el uso indebido de los modelos. Como resultado, muchas organizaciones pueden certificar la conformidad sin comprender realmente los riesgos relacionados con la IA.

Los marcos como NIST AI RMF e ISO/IEC 42001 proporcionan una orientación, pero son su implementación y su aplicación lo que garantiza realmente el cumplimiento. Cada sistema de IA es un sistema de datos antes que un sistema de información. Si los líderes no pueden identificar sus flujos de datos, sus rutas de uso indebido y sus modos de fallo, el sistema no está preparado para la escalabilidad.

> “Cada vez que se automatiza la toma de decisiones, se repite un mismo patrón: los resultados se mueven más rápido que las responsabilidades. La IA no crea esa brecha, la expone. Cuando las responsabilidades no están claras, **la gobernanza se vuelve simbólica**, por muy adecuada que parezca la política”.
>
> Joe Sullivan, exdirector de seguridad, Uber

Shadow AI es shadow IT a velocidad de las máquinas.

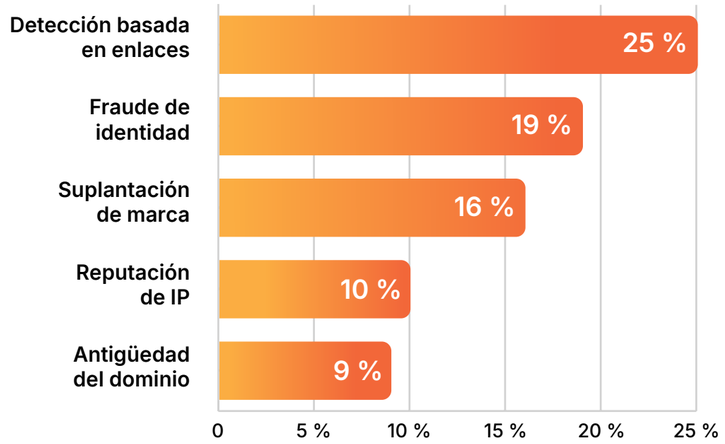
La IA puede proliferar sin ser detectada entre los empleados, los contratistas, los equipos de productos y los proveedores externos sin desencadenar ninguna revisión formal. Esto crea una brecha de auditabilidad precisamente cuando los reguladores exigen una mayor transparencia.

Los gobiernos y los reguladores exigen cada vez más a las empresas inventarios de IA documentados, trazabilidad de los datos y explicabilidad de las decisiones automatizadas. La incapacidad de demostrar el control se está convirtiendo rápidamente en un incumplimiento, no solo en un problema de madurez.

Las organizaciones líderes que están subsanando esta brecha están evolucionando de las auditorías esporádicas a la garantía continua, combinando el registro integral, la recopilación automatizada de pruebas y los controles que detectan el uso no autorizado de la IA en tiempo real.

Si la actividad de la IA no se puede registrar, explicar y demostrar con pruebas, no se puede defender ante los reguladores, los clientes o el consejo de administración.

Principales categorías de amenazas en la detección de correo electrónico



Los porcentajes no suman el 100 %, ya que los correos electrónicos pueden corresponder a varias categorías de amenaza.

Fuente: Cloudflare Radar

Los ataques basados en enlaces y el robo de identidad dominan las amenazas modernas por correo electrónico. Estas campañas explotan las señales de confianza en lugar de las vulnerabilidades técnicas. La IA reduce el coste de los métodos para llevar a cabo fraudes convincentes y personalizados, y la gobernanza debe ir más allá de la supervisión del modelo e incluir la autenticación, la integridad de la identidad y la trazabilidad de las decisiones.

> La gobernanza suele parecer suficiente **hasta que ocurre algo inesperado**. Con la IA, ese momento llega antes y con un impacto más amplio. Las organizaciones que sortean este desafío consideran la IA menos como una herramienta y más como una cadena de suministro (rastreando su origen, su propiedad y su influencia, incluso cuando está ubicada externamente)".
>
> Kate Kuehn, directora global de estrategia de ciberseguridad, World Wide Technology

La regulación reside en el código, no solo en las políticas.

En todo el mundo, las jurisdicciones han avanzado con decisión hacia regímenes de gobernanza de la IA aplicables que equilibran la innovación con la responsabilidad. Solo en Estados Unidos, los legisladores estatales presentaron 1208 proyectos de ley relacionados con la IA, lo que dio lugar a la promulgación de 145 nuevas leyes en un solo año.[3] Las sanciones van más allá de las multas y abarcan la exposición personal y fiduciaria.

Esto indica un cambio más amplio: la gobernanza de la IA se está replanteando como un riesgo empresarial y una responsabilidad del equipo directivo, y no como una política técnica discrecional. Las organizaciones que diseñan la gobernanza de la IA como infraestructura hacen de la confianza un factor de crecimiento, no una limitación.

> Presenciamos la mayor proliferación de Shadow IT de la historia, a medida que los empleados adoptan servicios y agentes de IA no controlados. A diferencia de la Shadow IT tradicional de SaaS, estas funciones de IA son difíciles de detectar o bloquear; pueden asumir identidades de usuarios reales, integrarse en la actividad estándar y operar a velocidad de las máquinas. El cometido del CISO no es bloquear esta adopción, sino diseñar funciones de IA seguras que eliminen la necesidad de herramientas no controladas".
>
> Michael Goodman, vicepresidente/director digital y de seguridad (CD y SO), Hitachi

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Exponer los puntos ciegos de la gobernanza de la IA

La velocidad de las máquinas, la propiedad poco clara, la visibilidad limitada y las medidas de protección débiles se convierten en responsabilidades empresariales, por lo que estas cuestiones son imperativas para los directivos.

P1

¿Quién es formalmente responsable de la gobernanza de la IA a nivel ejecutivo?

¿Dónde empieza y acaba esa autoridad? ¿Esta responsabilidad se implementa o bien se asume hasta que algo falla?

P2

¿Qué limitaciones definen hoy en día el comportamiento aceptable de la IA en nuestra organización?

¿Están esas restricciones claramente expresadas y son explícitas, aplicables y coherentes en todos los equipos?¿O dependen en gran medida de la confianza en que nuestros equipos de trabajo cumplan las políticas?

P3

¿Cómo determinamos si el uso de la IA es adecuado, no solo conforme a la normativa?

¿Los usos de la IA cumplen la normativa, pero no están alineados con la intención, la ética o la tolerancia al riesgo de la empresa? ¿Regulamos los resultados, o solo el acceso y las herramientas? ¿Cómo identificamos un comportamiento conforme a la normativa y uno no conforme?

P4

Si mañana nos auditaran, ¿podríamos mostrar un inventario completo y compartido del uso de la IA en toda la empresa?

¿O bien las definiciones, el uso no autorizado y la exposición relacionada con terceros pondrían de manifiesto que no disponemos de los conocimientos suficientes?

P5

Al acelerarse la adopción de la IA, ¿nuestro modelo de gobernanza sigue siendo coherente?

¿O bien está dividido según las funciones, los proveedores y las regiones? ¿Se considera la gobernanza como un marco estático o como un sistema operativo dinámico?

2

La confianza a la velocidad de las máquinas: desarrollar para la autonomía

La confianza a la velocidad de las máquinas: desarrollar para la autonomía

Las empresas emprenden ahora su transformación más importante desde la aparición del Internet comercial. Hemos pasado de las herramientas asistidas por IA a la era de la "empresa autónoma", donde los agentes de IA y los flujos de trabajo agénticos ejecutan procesos empresariales integrales con una intervención humana mínima o nula. Este desafío asume que los sistemas de IA ya están integrados y actúan de forma autónoma. A diferencia del desafío de la gobernanza de la IA, que se centra en la visibilidad, la supervisión y la responsabilidad, este desafío aborda lo que sucede una vez que la autoridad ya se ha delegado a las máquinas. La cuestión ya no es dónde se utiliza la IA o quién es el responsable, sino si la confianza está justificada cuando se toman decisiones sin intervención humana.

Gartner prevé que, para 2026, se espera que casi la mitad de las aplicaciones empresariales incorporen agentes de IA para tareas específicas, en comparación con la adopción de un solo dígito un año antes.[4] Este cambio ofrece una velocidad y una eficiencia sin precedentes, al mismo tiempo que plantea un riesgo estructural: la velocidad de las decisiones empresariales supera ahora la de la supervisión humana.

La confianza ya no puede ser periódica, manual o retrospectiva. En un entorno autónomo, la confianza debe ser continua, verificable y aplicada a la velocidad de las máquinas. Proteger este futuro requiere un cambio fundamental: las empresas deben evolucionar del principio de "confiar pero verificar" al de "confianza por diseño" y, en última instancia, a sistemas cada vez más fiables a medida que se prueban.

La "paradoja de la velocidad": cuando la empresa evoluciona más rápido que la supervisión

La seguridad tradicional requiere tiempo. Se genera una alerta. Un usuario humano investiga. Se toma una decisión. Los sistemas autónomos eliminan ese intervalo. Los agentes de IA pueden ejecutar miles de acciones, como reconfigurar la infraestructura, reequilibrar las carteras y ajustar las cadenas de suministro, en cuestión de milisegundos. Si un agente está comprometido, desalineado o simplemente equivocado, las consecuencias se producen antes de que un usuario humano pueda intervenir.

Esta es la paradoja de la velocidad: la misma autonomía que genera valor también reduce el margen de error. Los atacantes entienden esta situación. El phishing, la suplantación y la manipulación basados en la IA se dirigen cada vez más a los flujos de trabajo automatizados en lugar de a personas.

La implicación es clara: la seguridad no puede estar fuera del sistema. Debe estar integrada en la propia capa de decisión, regulando la intención, no solo el acceso. Este desafío no está relacionado con la predicción de los ataques. Se trata de garantizar que, cuando tus propios sistemas actúen, lo hagan dentro de los límites diseñados intencionadamente por el equipo directivo.

El nuevo plano de control para la IA autónoma

1. La identidad debe ir más allá de los usuarios humanos

Las identidades no humanas (los agentes de IA, las cuentas de servicio, los bots) ahora superan considerablemente en número a los usuarios humanos. Los bots son responsables de aproximadamente el 30 % del tráfico HTTP que entrega Cloudflare,[5] y un 92 % de todos los intentos de inicio de sesión observados por Cloudflare proceden de bots, a menudo ataques de relleno de credenciales.[6] Sin embargo, la mayoría de las empresas siguen regulando la identidad como si las personas fueran los actores principales.

El riesgo es grave. Los sistemas de IA se implementan con frecuencia sin una autenticación sólida, una autorización basada en el alcance o controles del ciclo de vida. Cuando se ven vulnerados, el alcance del impacto es tan amplio como el de una máquina.

Todos los agentes de IA deben tener una identidad criptográfica verificable, regulada a través de la gestión de identidad de las máquinas. Las credenciales deben tener una duración limitada, depender del contexto y ser revocables en tiempo real. La autonomía sin identidad significa la abdicación.

Distribución de solicitudes HTTP de bots (automatizadas) vs. de usuarios humanos

Fuente: Cloudflare Radar

Ya no operamos en un Internet centrado en los usuarios humanos. Los algoritmos interactúan cada vez más entre ellos, a menudo sin supervisión humana directa. Los modelos de gobernanza creados en torno a la autenticación de los usuarios y los controles de acceso de los empleados no se ajustan a esta realidad.

2. Los sistemas probabilísticos requieren medidas de protección deterministas

Los sistemas de IA razonan probabilísticamente. La seguridad no puede hacerlo. Aunque los agentes pueden realizar tareas de optimización, negociación o recomendación, las reglas que rigen lo que pueden hacer deben ser absolutas. Las políticas no se pueden inferir, se deben aplicar.

Esto requiere:

- Una política como código que defina restricciones no negociables
- Capas de aplicación en tiempo real que intercepten la intención antes de la ejecución
- La separación entre la toma de decisiones y la autorización

Solo existe una verdadera autonomía cuando los límites son explícitos, se aplican, y se diseñan de antemano.

> El criterio humano aún es fundamental, pero ya no opera a la velocidad que requieren los sistemas. En entornos donde las máquinas interactúan continuamente, **la confianza tiene que ser asumida, aplicada y verificada por diseño**, al igual que los sistemas de seguridad en los que confiamos sin darnos cuenta, hasta que fallan".
>
> Oliver Newbury, asesor sénior, TPG

3. La confianza requiere observabilidad, no suposiciones

A medida que los sistemas de IA se adaptan, se desvían y aprenden, lo que ayer era una certeza hoy es rápidamente irrelevante. Sin una observabilidad profunda, los responsables no pueden distinguir entre el comportamiento autónomo legítimo y la manipulación.

El uso no autorizado y a menudo invisible de la IA agrava aún más el riesgo, al introducir en las operaciones básicas modelos, flujos de datos y lógica de decisiones no regulados.

El argumento económico

La integración de la IA y la automatización en las operaciones de seguridad genera beneficios económicos cuantificables. Las organizaciones que utilizan estas funciones de forma generalizada resuelven las vulneraciones de seguridad 80 días más rápido y reducen el coste medio de las vulneraciones de seguridad en 1,9 millones de dólares en comparación con las que no lo hacen.[7]

La ventaja va más allá de la reducción de costes. Con unas medidas de protección eficaces, los responsables adquieren la confianza necesaria para implementar la automatización más profundamente en sus flujos de trabajo críticos para los ingresos y mejorar su capacidad de respuesta, su velocidad para generar ganancias y su diferenciación competitiva. Una autonomía bien regulada es un factor de crecimiento, no solo un control de riesgos. La seguridad a velocidad de las máquinas no es una sobrecarga. Es el resultado de ampliar la autonomía sin puntos débiles.

El sistema de liderazgo para la autonomía

El auge de los sistemas autónomos está redefiniendo el papel del CISO y, por extensión, las responsabilidades de todo el equipo directivo. El liderazgo en seguridad ya no consiste en proteger los sistemas una vez tomadas las decisiones; se trata de orquestar la confianza en entornos donde las máquinas actúan de forma independiente.

Un CISO recordaba la primera vez que un sistema de IA detuvo una transacción multimillonaria por sí solo. La decisión era correcta, pero suscitó una pregunta más importante en la sala de juntas: ¿quién había autorizado realmente a la máquina a tomar esa decisión? La tecnología se había adelantado a la gobernanza.

Este cambio exige decisiones ejecutivas claras: dónde se permite la autonomía, dónde los humanos siguen participando, qué transparencia se requiere en los modelos y los datos, y cómo se mide el riesgo cuando las máquinas toman decisiones.

Las métricas creadas para los tiempos de respuesta de los usuarios humanos ya no son suficientes. Los responsables deben hacer un seguimiento del riesgo autónomo, la integridad de las decisiones y la deriva sistémica. Sin embargo, solo alrededor del 15 % de los consejos de administración de las empresas reciben periódicamente métricas de riesgo y rendimiento relacionadas con la IA.[8]

Con la propagación de la autonomía, la seguridad, el cumplimiento y la tecnología ya no pueden operar de forma aislada. La seguridad influye en la velocidad de los ingresos. El cumplimiento determina el acceso al mercado. La tecnología define las responsabilidades. La confianza a la velocidad de las máquinas no es un programa de seguridad. Es un sistema de liderazgo que unifica la resiliencia, la gobernanza, la innovación y la reputación bajo un cometido del equipo ejecutivo.

> **La automatización cambia la velocidad de las decisiones, pero también cambia el alcance de los errores. La pregunta que se plantean los líderes es: "¿Cómo integramos la responsabilidad y la confianza en sistemas que actúan por sí solos?"**
>
> **Kevin Jones, director global de seguridad de la información, Bayer**

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Pasar de la automatización a la autonomía

Estas preguntas exponen si los directivos han diseñado intencionadamente límites en torno a cómo se toman las decisiones a la velocidad de las máquinas, y cómo se asume el riesgo en tiempo real.

P1

¿Qué decisiones empresariales ya toman los sistemas autónomos?

¿Qué decisiones reservamos deliberadamente para los usuarios humanos? ¿Está ese límite diseñado, documentado y revisado, o bien está implícito y es variable?

P2

Cuando las máquinas actúan por sí solas, ¿quién es responsable en tiempo real (el propietario del sistema, el propietario de la empresa o el patrocinador ejecutivo)?

¿La responsabilidad del riesgo autónomo está claramente definida durante el funcionamiento del sistema o bien solo se analiza cuando algo falla?

P3

¿Dónde las decisiones las ejecuta el software y no las personas?

¿Dónde hemos relajado los controles sobre el software? ¿Se exige más a las máquinas que a los humanos o bien se confía más en ellas?

P4

¿Podemos explicar y justificar una acción autónoma cuando se produce?

¿O bien tardamos días, hasta que revisamos el incidente posteriormente? ¿La intención es observable a la velocidad de las máquinas o se puede reconstruir en situaciones difíciles?

P5

¿Nuestro modelo de confianza se puede ampliar a la velocidad de las máquinas?

Si la autonomía se duplicara en el próximo año, ¿nuestro modelo de confianza podría o no absorber la aceleración? ¿La confianza está diseñada para la escala y la velocidad, o bien es heredada de la gobernanza de la era humana?

3

Cadenas de suministro en la sombra: exponer las dependencias ocultas

Cadenas de suministro en la sombra: exponer las dependencias ocultas

Nuestra economía hiperconectada ya no se define por lo que controlas, sino por lo que puede arruinarte y de lo que ni siquiera eres consciente. Muchos líderes han reforzado su perímetro, modernizado su infraestructura y reforzado su gobernanza, pero los riesgos más importantes ahora están más allá de su línea de visión, integrados en ecosistemas de terceros, de cuarta parte y de otros proveedores, de los que no son propietarios y sobre los que no tienen el control. La incómoda verdad: tu empresa puede ser madura desde el punto de vista operativo pero sistemáticamente frágil.

Las cadenas de suministro en la sombra no son casos extremos; son el resultado natural de la combinación de sistemas digitales a gran escala. Cada integración SaaS, llamada API, biblioteca de código abierto y servicio de IA añade otra capa de riesgo heredado. La pregunta que debe plantearse el equipo directivo ya no es "¿Tenemos riesgos relacionados con la cadena de suministro?" sino "¿Entendemos qué fallo externo podría mañana mismo frenar nuestros ingresos, erosionar la confianza o desencadenar el escrutinio normativo?"

El impacto ya es importante. Las fugas de la cadena de suministro representan de promedio 4,91 millones de dólares, una cifra superior al promedio global de fugas de 4,44 millones de dólares.[9] La opción estratégica para los líderes empresariales es considerar el riesgo relacionado con la cadena de suministro como un tema de cumplimiento y aceptar imprevistos periódicos, o considerarlo como una exposición operativa en tiempo real que exige una visibilidad continua, una garantía de ejecución y medidas de protección de la arquitectura.

El riesgo que nunca se aprobó

Las cadenas de suministro modernas ya no se detienen en los proveedores directos. Se extienden a las plataformas SaaS, los servicios nativos de nube, los proveedores de modelos de AI, los componentes de código abierto y las capas de infraestructura subcontratadas que operan mucho más allá del ámbito de supervisión del equipo de compras. Los fallos en cualquier lugar de esta red ampliada (ya sea una fuga, una interrupción o un incumplimiento) pueden desencadenar rápidamente perjuicios para los clientes, exponer a la empresa a riesgos relacionados con el cumplimiento normativo e causar interrupciones sistémicas.

El principal desafío es la visibilidad, y la IA acelera tanto los riesgos como la opacidad. La mayoría de las organizaciones no pueden ver sus cadenas de suministro digitales ampliadas, y mucho menos controlarlas en tiempo real. Cada modelo de IA, cada API y cada flujo de trabajo automatizado amplía las dependencias más allá de la supervisión tradicional. Las auditorías son estáticas, mientras que el riesgo es dinámico.

Cuando los sistemas se combinan y no se construyen

Un coche moderno lo fabrican cientos de proveedores, y las piezas de hardware, los chips y el software provienen de muchos proveedores, cada uno con sus propias cadenas de suministro. Un pequeño defecto oculto puede convertirse en un verdadero problema de seguridad cuando el vehículo circula por una autopista. Por este motivo, los fabricantes de automóviles invierten mucho en la trazabilidad y las pruebas continuas.

La informática empresarial refleja ahora este modelo. Una aplicación puede depender de decenas de herramientas SaaS, servicios en la nube, API, bibliotecas de código abierto y modelos de IA, cada uno con subprocesadores subyacentes. La empresa ve la interfaz, no las capas subyacentes. Esa es la cadena de suministro en la sombra.

La diferencia es la disciplina. En el sector de la automoción, el seguimiento de las piezas está garantizado y las retiradas se realizan con precisión. En el sector de las tecnologías de la información, cuando una biblioteca o un componente de IA se ve vulnerado, muchas organizaciones se apresuran a verificar si están afectadas por esta exposición. Los cuestionarios anuales no pueden seguir el ritmo de sistemas que cambian cada semana. La visibilidad y la garantía continua son ahora tan esenciales para los sistemas digitales como el control de calidad para los automóviles.

Tres fuerzas aceleran este riesgo:

- **La confianza por representación se ha convertido en el modelo operativo por defecto.** Las empresas confían en sus proveedores. Los proveedores confían en sus suministradores. Pocas partes verifican toda la cadena. Las preocupaciones acerca de la competencia y una visibilidad interna limitada hacen que las cadenas de suministro secundarias rara vez se describan en detalle.
- **La IA ha introducido una nueva capa opaca de dependencia.** Los empleados dependen cada vez más de las herramientas de IA generativa y de los servicios de IA integrados que exponen los datos confidenciales a modelos de cuarta parte. Los equipos de gestión de riesgos de terceros a menudo no tienen claro cómo estos modelos utilizan los datos, retienen la información o se entrenan con los datos de la empresa, lo que aumenta los riesgos relacionados con el cumplimiento normativo, la propiedad intelectual y la soberanía de los datos.
- **Las expectativas en materia de normativa se están endureciendo.** En todo el mundo, los reguladores están pasando con decisión de la simple orientación a la aplicación estricta de las normativas. Las autoridades esperan cada vez más que las organizaciones demuestren su visibilidad de las dependencias de terceros y de cuartas partes, especialmente cuando se trata de datos personales o financieros o de infraestructuras esenciales. En el futuro, se espera que los líderes no solo evalúen el riesgo relacionado con los proveedores, sino que cuantifiquen el riesgo operativo derivado de las cadenas de suministro ampliadas. ¿El resultado? Una brecha cada vez mayor entre lo que esperan los reguladores y lo que las organizaciones pueden demostrar actualmente.

Las 10 marcas más suplantadas en campañas de phishing

1	Windows	6	Amazon
2	SANS	7	Instagram
3	Microsoft	8	Costco
4	Stripe	9	YouTube
5	Facebook	10	iCloud

Fuente: Intentos de suplantación observados por Cloudflare Email Security

Las marcas más suplantadas no son objetivos aleatorios. Son plataformas esenciales integradas en los flujos de trabajo empresariales: proveedores de identidad, sistemas de pago, plataformas en la nube, sistemas operativos. Los atacantes aprovechan la familiaridad y la dependencia, convirtiendo una infraestructura digital de confianza en un vector de ataque. Las cadenas de suministro en la sombra no son solo un riesgo operativo; exponen también la identidad y la imagen de la marca.

De la garantía estática a la transparencia continua

La resolución del problema de la cadena de suministro en la sombra no requiere más formalidades documentales. Requiere un modelo operativo distinto. El futuro de la seguridad de la cadena de suministro es la transparencia continua: visibilidad en tiempo real de los procesos que realmente se ejecutan, se conectan e intercambian datos en todo el ecosistema.

Un CISO relató haber identificado un proveedor esencial solo después de que apareciera tráfico inusual en los registros de red. El proveedor era legítimo, pero nadie se había dado cuenta de lo estrechamente integrado que estaba. La lección era sencilla: no se puede regular lo que no se puede ver.

Este cambio ya está en marcha. Las listas de materiales de software (SBOM) y el formato Vulnerability Exploitability eXchange (VEX) están pasando de ser artefactos de cumplimiento a señales operativas. Debemos esperar que cada vez con más frecuencia el equipo de compras requiera no solo contratos, sino también informaciones declarativas en tiempo real y legibles por máquina que correlacionen los componentes, las dependencias y los datos relacionados con las vulnerabilidades a medida que estos cambien.[10]

Al mismo tiempo, las medidas de control se aplican cada vez más cerca de donde se manifiesta el riesgo. Los controles de las capas de red y de conectividad permiten a las organizaciones observar el comportamiento, detectar los flujos de datos no autorizados e identificar los proveedores en la sombra en el mismo momento en que se desarrolla la actividad.

La seguridad de la cadena de suministro ahora es una función operativa, en lugar de una revisión periódica. La confianza se verifica siempre. El riesgo se detecta pronto. La gobernanza avanza al mismo ritmo que el ecosistema que debe proteger.

Confiar, pero verificar siempre

El 30 % de las fugas en 2025 estuvieron relacionadas con la participación de terceros, el doble que el año anterior[11]. Esto demuestra hasta qué punto las relaciones de la cadena de suministro influyen ahora en la exposición a riesgos más allá de los límites internos tradicionales.

Sin embargo, las organizaciones líderes comparten un patrón común: consideran el riesgo relacionado con la cadena de suministro como un sistema, y no como una función de cumplimiento. Insisten en saber qué aplicaciones existen y cómo se conectan. Requieren transparencia a lo largo de la cadena de suministro y no se detienen en el primer contrato. Utilizan señales a nivel de red para detectar la actividad paralela en lugar de depender de la autocertificación. Aplican los principios Zero Trust al acceso entre máquinas, no solo a los usuarios. Y reevalúan continuamente el riesgo relacionado con los proveedores en función del comportamiento, no de la reputación.

Las ventajas son tangibles. El 85 % de las organizaciones líderes en modernización de aplicaciones están eliminando activamente las herramientas redundantes y la Shadow IT para reducir la superficie de ataque de su cadena de suministro y mejorar su velocidad operativa.[12] No se trata de ajustes técnicos. Son decisiones del equipo directivo sobre cuánta incertidumbre una organización está dispuesta a tolerar en los sistemas de los que depende cada día.

> El riesgo rara vez proviene de las dependencias que todo el mundo espera, sino **de las que nadie puede ver**. Cuando la visibilidad es incompleta, las auditorías ofrecen tranquilidad, pero poca protección. La verdadera resiliencia proviene de arquitecturas que revelan sus dependencias durante su funcionamiento".
>
> Tim Brown, director de seguridad de la información, SolarWinds

> **Los ecosistemas interconectados recompensan la velocidad y la especialización, pero también distribuyen el riesgo de una forma que los contratos no permiten representar. La información operativa, no las formalidades documentales, es lo que en definitiva contiene la exposición al riesgo".**
>
> **Sandip Wadje, responsable global de riesgos operativos e información de tecnologías emergentes, BNP Paribas**

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Regular el riesgo que no controlas

El riesgo relacionado con la cadena de suministro ya no se puede gestionar. Es una realidad que las organizaciones deben aceptar. Determina si ese riesgo es visible y está regulado, o bien si es opaco y está asumido.

P1

¿Qué procesos empresariales esenciales deberíamos detener si fallara una dependencia fundamental?

¿Sabríamos a qué se ha debido el fallo? ¿Podríamos asociar, en tiempo real, el impacto sobre los ingresos y los clientes con dependencias específicas?¿O bien solo descubriríamos las vulnerabilidades después del incidente?

→

P2

¿Cómo responderemos a las preguntas de los organismos reguladores o de los consejos de administración acerca de los riesgos del ecosistema?

¿Podemos responder las preguntas sobre estos riesgos sin hacer referencia a un contrato? ¿Tenemos visibilidad técnica sobre la ruta operativa del riesgo relacionado con los proveedores?

→

P3

¿Dónde hemos reducido la visibilidad en la cadena de suministro para priorizar la velocidad, la comodidad o las relaciones con nuestros proveedores?

¿Estas elecciones han sido deliberadas? ¿Quién ha decidido aceptar esas concesiones? ¿Qué dependencias están definitivamente "fuera de los límites" del escrutinio?

→

P4

¿Con qué rapidez podemos determinar si una nueva vulnerabilidad identificada nos afecta?

¿Están claramente asignadas las responsabilidades relacionadas con la respuesta? ¿La detección de la exposición requiere minutos, días o semanas?

→

P5

¿Gestionamos el riesgo relacionado con la cadena de suministro como una disciplina continua o como una auditoría periódica?

¿Nuestro modelo evoluciona al mismo ritmo que nuestro ecosistema, o bien simplemente nos confirma que los controles del año pasado se han revisado?

4

Señales de intención: de la información a la previsión

Señales de intención: de la información a la previsión

Si echas un vistazo a los titulares, verás que la proliferación de las actividades de los ciberdelincuentes continúa, a una velocidad y una escala cada vez mayores. Con el reconocimiento y los kits de herramientas asistidos por IA, aumenta el número de ciberdelincuentes capaces de perpetrar ataques mayores y más sofisticados que nunca. Además, el intervalo entre la aparición de la amenaza y el impacto en la empresa es cada vez más breve, ya que el tiempo medio que tarda un ciberdelincuente en empezar a moverse lateralmente se ha reducido a solo 48 minutos.[13]

La información sobre amenazas, que antes se consideraba una función opcional, ahora es esencial. Hoy en día, el 52 % de las organizaciones cuentan con equipos internos dedicados a la información sobre ciberamenazas.[14] En el panorama de las amenazas en rápida evolución, esta información ha pasado de ser una función de seguridad a una capacidad de liderazgo. El éxito se mide por la capacidad de analizar los datos de la información sobre ciberamenazas en un contexto empresarial, descifrando las señales entre el ruido y convirtiendo el conocimiento en una previsión práctica.

La finalidad de la información sobre amenazas ya no es saber más. Se trata de saber lo que importa, *con la antelación suficiente para actuar.*

De la información táctica a las señales estratégicas

Las amenazas modernas son muy rápidas, de mucho volumen y cada vez están más determinadas por la geopolítica, los incentivos económicos y las vulnerabilidades específicas de cada sector. En este entorno, la información sobre amenazas ya no puede considerarse como una función de seguridad opcional ni limitarse a revisiones de listas de comprobación de fuentes externas genéricas. El contexto (empresarial, sectorial y mundial) es importante, y los ejecutivos deben exigir información que relacione directamente las actividades de amenaza con el impacto empresarial, la exposición operativa y el riesgo estratégico.

Simplemente hay demasiada actividad en el frente de los atacantes como para estar al tanto de todo. La defensa requiere velocidad y competencias, y ambas suelen escasear. Si bien tu estrategia de seguridad debe abordar y reconocer el inventario completo de activos y pasivos bajo tu protección, el uso de la información sobre amenazas para comprender no solo los aspectos técnicos de las amenazas, sino también su contexto, te permite ajustar tu programa de seguridad para priorizar la reducción del riesgo en aquellas áreas que tienen un mayor impacto en tu organización.

Decidir qué es importante para la organización suele implicar la alineación del consejo de administración y el equipo directivo sobre cómo integrar los principios empresariales básicos, las fuerzas del mercado, las normativas y las aportaciones de las partes interesadas. Este contexto es muy útil a la hora de evaluar la información sobre amenazas, ya que proporciona el contexto que la empresa necesita para determinar qué datos de la información sobre ciberamenazas son más útiles.

De esta forma, la información sobre amenazas se puede utilizar para "silenciar" la información superflua (las vulnerabilidades irrelevantes o los grupos de atacantes que tienen como objetivo específico otros sectores) para que puedas centrar tus recursos donde puedan tener el mayor impacto en función del panorama de amenazas específico de tu organización. La información sobre amenazas que no forma parte de las decisiones ejecutivas es simplemente "ruido" que debe silenciarse.

Principales sectores objetivo de ataques DDoS en 2025

Clasificación	Sector
1	Apuestas y videojuegos
2	Telecomunicaciones
3	Servicios y tecnología
4	Servicios bancarios y financieros
5	Comercio minorista

Esta clasificación es un promedio de los ataques DDoS observados en todo el mundo en la capa de red y en la capa de aplicación. Tecnología y servicios ocupa el primer puesto en cuanto a los ataques a la capa de red. Videojuegos y apuestas ocupa el primer puesto en cuanto a los ataques a la capa de aplicación.

Fuente: Cloudflare Radar

La actividad de los ataques no se distribuye de forma uniforme. Los adversarios priorizan los sectores vinculados a una ventaja económica, la estabilidad de la infraestructura y la relevancia geopolítica. La concentración en sectores específicos refleja la intención estratégica, no la aleatoriedad. Una información eficaz prevé dónde se intensificará la presión, y adapta las defensas en consecuencia.

La información sobre amenazas ya no es negociable

A medida que la información sobre amenazas madura, deja de centrarse en los indicadores técnicos para priorizar la relevancia empresarial. Los ejecutivos recurren ahora a ella para determinar qué amenazas son realmente importantes, cómo los cambios geopolíticos y del sector afectan a la exposición, y dónde existen puntos débiles en el conjunto de las operaciones, los socios y los usuarios. La cuestión ya no es si la organización debe invertir en información sobre amenazas, sino qué tipo de información debe priorizar y pagar.

Para enmarcar las conversaciones presupuestarias, considera dónde la información sobre ciberamenazas proporciona el mayor valor a tu organización:

- **Validación** de que las inversiones en seguridad están alineadas con el perfil de riesgo de la organización
- **Reducción** del ruido operativo al centrar la protección en las amenazas más críticas
- **Reducción proactiva** del riesgo, frente a la respuesta reactiva a los incidentes después de que hayan producido

Para el director financiero, lo que justifica la información sobre amenazas no es el volumen de alertas, sino su capacidad para reducir la probabilidad y las repercusiones de una interrupción importante en las actividades empresariales (tiempo de inactividad, fraude, intervención normativa o daños a la reputación). De cara a la organización, esto exige claridad. Los acuerdos ad hoc y las funciones de información con recursos insuficientes no pueden proporcionar los conocimientos necesarios al equipo ejecutivo, ni los resultados esperados.

Tanto si se proporciona a través de un equipo interno, de socios de confianza o de un modelo híbrido, el cometido es el mismo: la información debe ser oportuna, contextual y relevante para la toma de decisiones. La información que solo explica lo que ocurrió ayer no contribuye apenas a proteger el mañana. Los proveedores que ofrecen una visibilidad novedosa, como una visión temprana de la infraestructura, la intención y la preparación del adversario, ofrecen una ventaja estructural.

> Los indicadores explican lo que ya ha ocurrido; la intención explica lo que viene a continuación. La información más útil conecta el comportamiento, el contexto y el motivo, **convirtiendo las señales aisladas en previsiones** en función de las que los líderes pueden tomar medidas antes de que se produzcan daños".
>
> **Menny Barzilay, cofundador y director general, Percepto**

Abordar el panorama de amenazas en 2026

Varios de los desafíos analizados en este capítulo se reflejan en el Informe sobre amenazas de Cloudflare 2026. Basado en datos de la red global de Cloudflare, que protege el 20 % de la web, el informe ayuda a los líderes empresariales a centrarse en los riesgos que requieren acción, no solo sensibilización.

Utiliza una perspectiva sencilla: el esfuerzo del atacante en relación con el impacto. Las amenazas más importantes son aquellas que generan un impacto empresarial descomunal sin apenas esfuerzo. En 2026, esto aparece en tres patrones.

- **La industrialización de los ataques:** el cambio del hackeo manual por la escalabilidad automatizada y fácil en toda la infraestructura de nube de una organización
- **Intrusiones que priorizan la identidad:** el ransomware pasa de ser un evento de intrusión a uno de inicio de sesión.
- **Conectividad de la cadena de suministro:** la utilización del tejido conectivo como arma entre los entornos SaaS y los entornos que priorizan las API.

Descarga el informe de Cloudflare sobre amenazas 2026.

Descargar informe

El ingrediente que falta: el modelado de amenazas

Si bien la integración de la información sobre amenazas en tus prácticas de seguridad permite optimizarlas en todos sus aspectos, la estrecha integración con el modelado de amenazas la lleva un paso más allá y la convierte en un motor estratégico empresarial.

Aunque cada vez más organizaciones tienen en cuenta el riesgo en la toma de decisiones e incluyen la reducción del riesgo en sus objetivos estratégicos a largo plazo, solo el 37 % de las organizaciones han formalizado y documentado con éxito sus procesos de modelado de amenazas.[15] El modelado de amenazas proporciona una taxonomía común que alinea al CISO, al equipo directivo y a la junta directiva en torno a supuestos de riesgo compartidos. Obliga a una definición clara de la priorización de los activos, la probabilidad de riesgo y el impacto en el negocio en caso de que fallen los controles.

La perspectiva que se obtiene en los ejercicios de modelado de amenazas es intencionadamente de alto nivel; los consejos de administración quieren claridad sobre el riesgo sistémico, las tendencias emergentes de las amenazas y si la organización está posicionada en el lado correcto del desafío de las amenazas. Mediante el modelado de amenazas, los riesgos inherentes se miden según la probabilidad y la gravedad del impacto, en función de las prioridades de la organización. Factores como los controles de seguridad y los resultados de las auditorías, junto con el análisis de la información sobre amenazas, proporcionan cálculos del riesgo residual.

La inyección de datos de la información sobre ciberamenazas en el proceso de modelado de amenazas facilita un mayor ajuste, y ofrece una base para actividades como la validación de controles y la detección de amenazas (ambas tareas esenciales en una postura de seguridad proactiva). Además, la información relevante del sector puede confirmar si las medidas de protección están reforzadas contra los adversarios más probables, y proporcionar a los responsables de la toma de decisiones indicadores eficaces para la planificación presupuestaria y estratégica.

Sin el modelado de amenazas, la información es puramente operativa. Con él, la información pasa a ser estratégica.

> La información adecuada reduce el ruido. Una información remarcable cambia las decisiones. La diferencia es si ayuda a los líderes a anticiparse a los movimientos, no solo a explicarlos".
>
> Troy Wilkinson, asesor de riesgo, YL Ventures

Solamente

el 37 %

de las organizaciones han formalizado y documentado con éxito sus procesos de modelado de amenazas.[16]

PREGUNTAS PARA EL EQUIPO DIRECTIVO

La información sobre amenazas como disciplina de liderazgo

La información sobre amenazas adecuada conecta la seguridad, el riesgo, las operaciones, las finanzas y la estrategia en una visión ejecutiva coherente de la exposición y la intención.

P1

¿Protegemos lo que conocemos o lo más relevante?

¿Hemos adaptado explícitamente nuestras medidas de protección a las amenazas que podrían interrumpir este año nuestros ingresos y nuestras operaciones o socavar la confianza depositada en nosotros?

P2

¿Con qué antelación podemos ver realmente la intención del adversario?

¿Dónde identificamos ataques por el daño causado y no por la información? ¿Estamos a la vanguardia o a la zaga del ciclo de las amenazas?

P3

¿Las sesiones informativas sobre amenazas determinan nuestras decisiones o solo permiten compartir información?

¿Esta información cambia, en tiempo real, nuestras prioridades, nuestra inversión o nuestra tolerancia al riesgo?

P4

¿Qué decisiones o procesos empresariales fallarían primero si una persona de confianza se viera comprometida?

¿Hemos diseñado flujos de trabajo suponiendo que el criterio humano puede ser manipulado o suplantado?

P5

¿Con qué rapidez podemos adecuar nuestras estrategias cuando los adversarios cambian las suyas?

¿De qué mecanismos disponemos que nos indiquen que se avecina un cambio antes de que la empresa lo perciba?

5

La trampa de la deuda: la arquitectura heredada como riesgo estratégico

La trampa de la deuda: la arquitectura heredada como riesgo estratégico

En 2026, la deuda técnica representa un riesgo empresarial importante que socava silenciosamente la competitividad. Las organizaciones ya estaban al límite en 2025, gestionando más de 130 vulnerabilidades nuevas cada día, casi el 40 % de las cuales se calificaron como de riesgo alto o crítico.[17] A medida que el uso de la IA como arma hace que las arquitecturas heredadas sean indefendibles, las organizaciones con pilas fragmentadas corren el riesgo de quedar atrapadas en un ciclo de seguridad reactiva, innovación limitada y exposición agravada.

La deuda técnica se ha convertido en una superficie de ataque expuesta, donde el riesgo se agrava tan rápido que supera la capacidad de respuesta de los equipos humanos. Aquellos que se modernicen con decisión no solo reducirán el riesgo, sino que también se beneficiarán de la velocidad, la confianza y la adaptabilidad necesarias para competir en la economía impulsada por la IA.

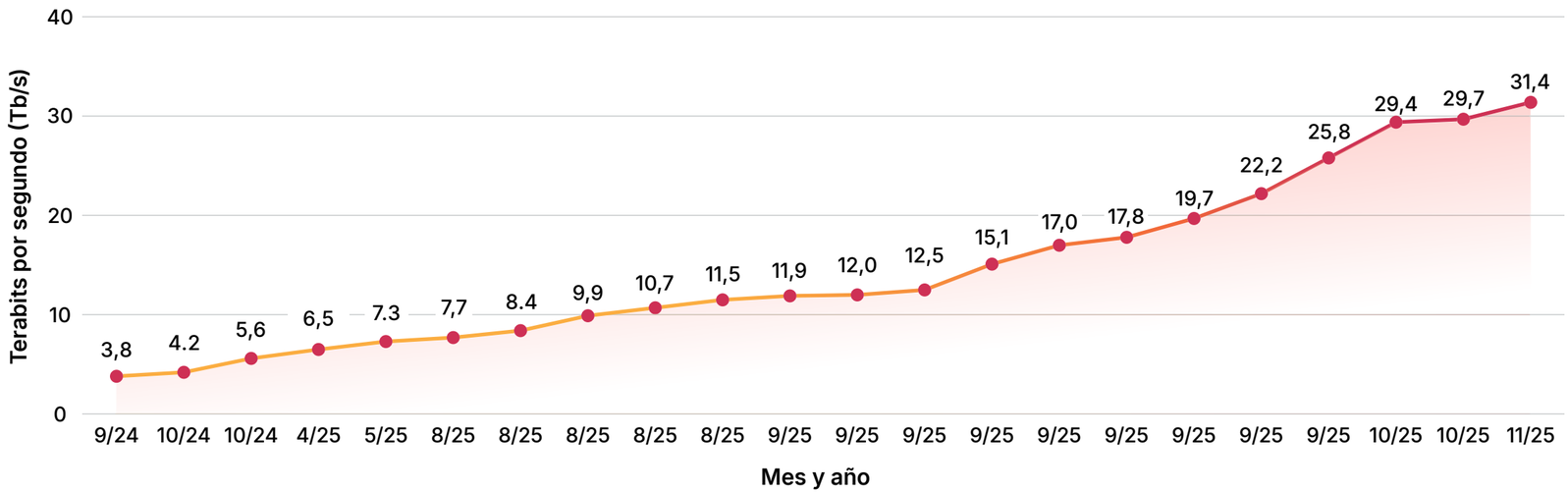
Cuando la velocidad expone la debilidad estructural

El cambio determinante de 2026 no es el volumen de vulnerabilidades, sino la velocidad a la que se explotan. La IA agéntica ha reducido aún más el intervalo entre la divulgación y la explotación. Esto permite a los ciberdelincuentes identificar las vulnerabilidades y poner en práctica su explotación en cuestión de días, y cada vez más, de horas.

Los datos son contundentes. En 2025, se observó la explotación activa de 884 vulnerabilidades, y el 29 % de ellas mostró indicios de explotación el mismo día de su publicación.[18] La escala es igualmente sin precedentes. React2Shell, una de las vulnerabilidades más destacadas del año, registró más de mil millones de intentos de explotación en solo 11 días.[19]

Escalada sin preparación de la arquitectura

Los mayores ataques DDoS jamas registrados en todo el mundo



Fuente: Cloudflare Radar

En poco más de un año, el mayor ataque DDoS registrado se multiplicó casi por diez. Los sistemas centralizados y estrechamente vinculados no se diseñaron nunca para esta escala. Ahora, la deuda técnica se traduce directamente en fragilidad sistémica bajo la presión de la velocidad de las máquinas.

Los entornos heredados no pueden soportar la presión. Los fallos importantes suelen producirse cuando las dependencias compartidas fallan al mismo tiempo. Años de soluciones rápidas han creado una deuda oscura: integraciones ocultas, API frágiles y sistemas donde la aplicación de revisiones es demasiado arriesgada. Estos entornos no se crearon para las amenazas a la velocidad de las máquinas ni para la verificación continua.

Esto también expone las limitaciones de los ciclos de revisiones de 30, 60 y 90 días. Las amenazas se explotan en horas, no en trimestres. La protección debe trasladarse al perímetro, y reducir la exposición antes de que los sistemas vulnerables se vean afectados.

> Los atacantes no distinguen entre los sistemas obsoletos y los nuevos; **buscan los puntos débiles**. La deuda técnica aumenta silenciosamente el número de esos puntos débiles hasta que la defensa se convierte en un juego de probabilidades".
>
> Jerry Perullo, fundador, Adversarial Risk Management

El ciclo de la falta de innovación

Las organizaciones con pilas tecnológicas obsoletas están atrapadas en un ciclo de falta de innovación. Cuanto más frágil es la infraestructura, mayor es el número de incidentes de seguridad. A medida que aumentan los incidentes, más presupuesto y talento se dedican al mantenimiento. El resultado es una capacidad de crecimiento cada vez menor.

La empresa global media desperdicia más de 370 millones de dólares al año debido a su incapacidad para modernizar eficazmente sus sistemas y sus aplicaciones heredados, obsoletos e ineficientes.[20] Los estudios estiman que aproximadamente el 31 % de los recursos tecnológicos se dedican a resolver la deuda tecnológica.[21] La verdadera innovación (nuevos productos, iniciativas de IA, automatización) recibe tan solo el 7 %. Esto no es estancamiento; es regresión.

Mientras que las empresas líderes utilizan la IA para acelerar la diferenciación, las empresas rezagadas pagan una "tasa de interés" cada vez mayor por el código obsoleto que limita la velocidad, la resiliencia y la opcionalidad estratégica.

Por qué las pilas heredadas fallan bajo la presión de la IA

La seguridad moderna presupone la automatización, la integración y el control en tiempo real. Los sistemas heredados asumen una intervención manual, configuraciones estáticas y una protección basada en el perímetro. Ese desajuste se está volviendo peligroso a medida que la IA cambia la economía tanto del ataque como de la defensa.

Las arquitecturas obsoletas tienen dificultades debido a la lentitud de la aplicación de las revisiones (que requiere mucho tiempo de inactividad), la visibilidad limitada de las API y los flujos de datos, las herramientas fragmentadas que no pueden coordinar la respuesta y la debilidad de las bases para las operaciones basadas en la IA. Esto a menudo obliga a un equilibrio entre el riesgo cibernético y el riesgo operativo. Los directores técnicos y los CISO ya están familiarizados con este conflicto, cuando deben decidir si aplicar revisiones que podrían interrumpir las actividades empresariales. El resultado es el retraso, y el retraso es precisamente lo que explotan las amenazas a velocidad de las máquinas.

Las organizaciones retrasan la adopción de la IA no porque no sean ambiciosas, sino porque su infraestructura no puede admitirla de forma segura. Sin embargo, los competidores con arquitecturas modernizadas permiten que las iniciativas de AI impulsen la modernización, y utilizan cargas de trabajo reales para justificar y acelerar la renovación de la arquitectura. Por ejemplo, al 62 % de las organizaciones líderes en innovación de aplicaciones les resulta "muy fácil" hacer un seguimiento de su nivel actual de cumplimiento de la seguridad, en comparación con el 35 % de las empresas que van con retraso.[22]

370 millones USD

desperdiciados al año debido a la incapacidad de modernizar eficazmente los sistemas y aplicaciones heredados obsoletos e ineficientes[23]

La brecha del liderazgo

La diferencia entre las empresas líderes y las rezagadas es la disciplina en la toma de decisiones. Las organizaciones que escapan de la trampa de la deuda toman decisiones difíciles desde el principio. Centralizan la autoridad en materia de modernización, alinean la seguridad con la resiliencia empresarial y consideran la arquitectura como un activo estratégico. El 73 % de las empresas "líderes" en modernización han centralizado la toma de decisiones en un grupo reducido de personas, en comparación con solo el 36 % de las empresas "rezagadas".[24] Quienes fracasan quedan atrapados en la parálisis que generan los comités, donde las vulnerabilidades avanzan más rápido que las decisiones y el riesgo se agrava mientras los planes se debaten infinitamente.

La deuda técnica a menudo refleja la deuda organizativa. La propiedad fragmentada, las responsabilidades poco claras y las decisiones diferidas generan la misma fragilidad en los modelos operativos y de liderazgo que existe en la infraestructura heredada. En 2026, ya no será posible sobrevivir a esa fragilidad.

Modernización como reducción de riesgos: recuperar tiempo

Escapar de la trampa de la deuda requiere ver la modernización como un cometido para la resiliencia, y no como un ciclo de actualización informática. La modernización disminuye el riesgo al reducir la superficie de ataque gracias a la consolidación. Esto facilita la automatización de la aplicación de revisiones y de la capacidad de respuesta, así como la viabilidad de la protección y las operaciones basadas en la IA a gran escala. Y no menos importante, reasigna los limitados recursos de ingeniería a tareas que aportan un gran valor a la empresa, en lugar de tener que dedicarlos a un mantenimiento interminable.

Las organizaciones que tienen éxito no se modernizan reconstruyendo todo; crean una base estable y unificada en la que la seguridad, el rendimiento y la innovación se refuerzan mutuamente. Con esa base, los sistemas se pueden perfeccionar, escalar y adaptar rápidamente, sin acumular nuevas capas de fragilidad.

El cambio necesario no es incremental. Exige la alineación de los directivos y la adopción de medidas decisivas. La arquitectura heredada debe considerarse como un riesgo empresarial cuantificado, no como un inconveniente técnico. La autoridad de decisión para la modernización debe estar centralizada. Las iniciativas de IA facilitan la renovación arquitectónica, no esperan a que se den las condiciones idóneas. La consolidación de las plataformas es necesaria para reducir la complejidad y restaurar la visibilidad.

En definitiva, la modernización consiste en recuperar tiempo: tiempo para innovar, tiempo para responder y tiempo para competir antes de que el riesgo agravado mine la ventaja.

73 %

de las empresas "líderes" en modernización han centralizado la toma de decisiones con un grupo reducido de personas, en comparación con solo el 36 % de las empresas "rezagadas".[25]

PREGUNTAS PARA EL EQUIPO DIRECTIVO

El coste agravado de la arquitectura heredada

La deuda técnica reduce la velocidad y la resiliencia. Muchas empresas gastan más en mantener el pasado que en construir el futuro.

P1

¿Qué capacidades empresariales se ven actualmente limitadas por la deuda técnica?

¿Quién es el responsable de estos riesgos y en qué plazo previsto?

P2

¿Qué porcentaje del gasto en seguridad se dedica al mantenimiento de la infraestructura heredada y qué porcentaje a mejorar la resiliencia?

¿Cuál es nuestra combinación de objetivos para los próximos 12-24 meses?

P3

¿Qué iniciativas prioritarias se retrasan debido a los límites de la arquitectura?

¿Qué ventajas en materia de ingresos, eficiencia o riesgos estamos aplazando como resultado?

P4

¿Cuáles son las tres principales iniciativas para reducir la deuda técnica este año?

¿Cómo mediremos los avances y cómo exigiremos responsabilidades a los líderes?

P5

¿Cuáles son los mayores obstáculos para reducir la deuda técnica?

¿Se trata de límites presupuestarios, déficit de competencias técnicas, prioridades contrapuestas o una propiedad poco clara? ¿Cuáles eliminaremos primero?

6

Espejismo en la nube: desvinculación del riesgo en cascada

Espejismo en la nube: desvinculación del riesgo en cascada

A medida que las empresas se consolidan en menos plataformas en la nube para avanzar más rápido, muchas aumentan el riesgo sistémico. Las estrategias de mononube simplifican las operaciones, pero concentran los dominios de fallo, mientras que la multinube se suele considerar como una casilla de verificación y no como una estrategia de resiliencia diseñada.

Las interrupciones recientes han llevado a un hecho ineludible: la resiliencia no está determinada por cuántas nubes utiliza una organización, sino por cómo falla su arquitectura. En 2026, los líderes deben ir más allá de la ideología de la nube y adoptar arquitecturas de resiliencia por diseño, creadas para contener los fallos, limitar el alcance y preservar la confianza en las situaciones difíciles.

Cuando la velocidad se convierte en fragilidad

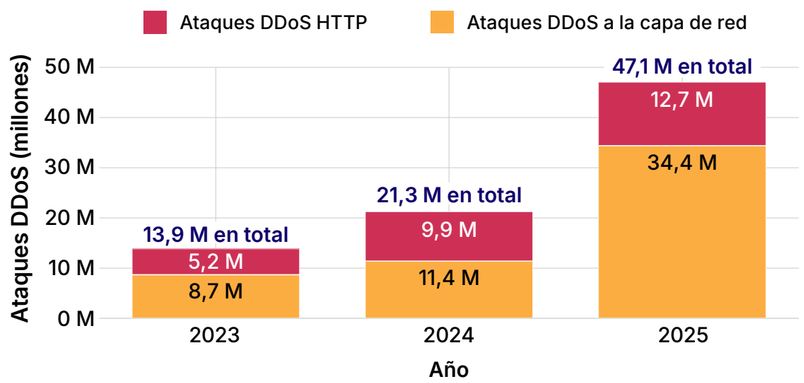
La empresa moderna no tenía la intención de desarrollar sistemas frágiles. La adopción de la nube prometía velocidad, elasticidad y fiabilidad, pero también presentaba un riesgo de concentración menos llamativo (menos visible, más sistémico y más difícil de resolver en condiciones difíciles).

Hoy en día, las interrupciones no se deben únicamente a fallos de un solo proveedor. Aunque el desencadenante puede seguir siendo un incidente de un solo proveedor, los eventos más graves se producen cuando fallan las dependencias compartidas en conjunto (sistemas de identidad, planos de control, canalizaciones de implementación y servicios de red que sustentan todo lo demás). Los datos plurianuales de Uptime Institute muestran que aproximadamente dos tercios de las interrupciones de las que se ha informado públicamente implican a proveedores externos de TI o de centros de datos, como gigantes de Internet y servicios de nube y empresas de telecomunicaciones y de colocación.[26]

Con demasiada frecuencia, la prioridad de la continuidad de las actividades empresariales es restaurar el servicio en lugar de evitar los fallos. Con el tiempo, las dependencias en capas convierten los entornos en sistemas estrechamente vinculados en los que los pequeños fallos pueden tener un efecto en cascada. Esta fragilidad solo suele salir a la luz en una situación de crisis.

Presión permanente

Ataques DDoS por año y tipo



Fuente: Cloudflare Radar

La actividad de DDoS se ha más que triplicado en dos años. Las interrupciones a gran escala ya no son incidentes puntuales, sino continuos. En entornos estrechamente vinculados, la presión externa continuada expone las dependencias ocultas e intensifica los pequeños fallos, que pasan a ser eventos sistémicos. La resiliencia debe asumir una presión constante, no un fallo ocasional.

> La nube crea escala, **pero no mejora automáticamente la resiliencia**. Si tus sistemas fallan a la vez, tu diseño no está preparado para la redundancia. Tienes un diseño para la correlación".
>
> **Mark Hughes, socio gerente global de servicios de ciberseguridad, IBM**

El lado positivo es claro. Las organizaciones que diseñan y prueban en busca de fallos obtienen resultados sustancialmente mejores. Una importante empresa de servicios financieros redujo un 40 % las interrupciones y casi un 60 % los tiempos de resolución tras modernizar su arquitectura, mejorar la observabilidad y diseñar para la preparación ante fallos.[27]

Hoy en día, las interrupciones no se deben tanto a fallos en la nube como a la erosión de la independencia. El riesgo real es el acoplamiento arquitectónico. La resiliencia requiere ahora un aislamiento intencionado, limitar el alcance y considerar la contención de fallos como un principio de diseño básico.

El espejismo de la mononube: eficiencia sin contención

Para muchas organizaciones, las estrategias de mononube se han convertido en la estrategia por defecto en su búsqueda de la eficiencia. Las herramientas estandarizadas reducen la complejidad, aceleran la implementación y reducen los costes operativos. La contrapartida es el riesgo de concentración. La misma consolidación que mejora la eficiencia también puede centralizar los fallos.

Los principales proveedores de nube suelen ser muy resilientes, pero hoy en día el mayor riesgo es arquitectónico y operativo. Cuando las canalizaciones de identidad, aplicación de políticas, observabilidad y entrega se basan en el mismo plano de control o límite de confianza, la resiliencia se convierte en una suposición y no en una propiedad integrada. Un único error, ya sea del lado del proveedor o del lado del cliente, puede propagarse ampliamente si el diseño no lo contiene. Puede que existan planes de recuperación, pero no suele haber una verdadera contención. Cuando algo falla, fallan demasiadas cosas al mismo tiempo.

Los datos del sector refuerzan esta realidad. Un estudio de Gartner muestra que la mayoría de los fallos en la nube se deben a errores de configuración y a problemas operativos, más que a defectos de la infraestructura principal. Los análisis basados en encuestas de Gartner atribuyen aproximadamente el 80 % de los fallos de seguridad en la nube a errores de configuración, y las previsiones sugerían que para el año pasado, hasta el 99 % de los fallos del entorno en la nube implicarían un error humano en algún punto de la cadena.[28] La lección no es que los humanos se equivoquen (siempre lo harán), sino que las arquitecturas deben estar diseñadas para absorber esos errores de forma segura.

La implicación práctica está clara. Es necesario diseñar para la resiliencia, no darla por sentada. Eso significa diseñar tanto para la contención como para la recuperación, separando las dependencias críticas, añadiendo medidas de protección y políticas como código para reducir el impacto de los errores, y probando periódicamente los escenarios de fallo. El riesgo de concentración no ha desaparecido en la era de la nube. Ha subido posiciones. Las organizaciones que siguen siendo resilientes son aquellas que garantizan que un único fallo no se convierte en un evento sistémico.

El mito de la multinube: redundancia sin independencia

La multinube se suele posicionar como el antídoto contra el riesgo de concentración. En la práctica, con frecuencia recrea la misma fragilidad, simplemente bajo distintos logotipos. La mayoría de los entornos multinube comparten proveedores de identidad, canalizaciones de CI/CD, herramientas de gobernanza y dependencias de SaaS. Cuando esas capas compartidas fallan, la promesa de independencia desaparece al instante. Esta es la razón por la que las revisiones posteriores a los incidentes revelan con tanta frecuencia que los sistemas "redundantes" nunca fueron realmente independientes.

La resiliencia no depende de cuántas nubes hay en un diagrama. Depende de qué capas fallan de forma independiente en una situación difícil, y cuáles no.

Diseñar para la contención, no para la perfección

El diseño autónomo parte de la expectativa de que los sistemas fallarán, y prioriza limitar los fallos y aprender de ellos. El objetivo no es solo resistir sus consecuencias, sino mejorar gracias a ellos.

Esto es posible gracias a la contención. Significa que un fallo en un área no se propaga automáticamente a otras. Un fallo aislado tiene un alcance limitado, una causa clara y un impacto controlable. No elimina la identidad, la política, los datos y las operaciones a la vez.

Las organizaciones que utilizan la IA y la automatización redujeron considerablemente la duración de los ciclos de vida de las vulneraciones de seguridad en **80 días**, así como el coste promedio de las vulneraciones de seguridad.

1,9 millones USD[29]

Esto se refleja en la arquitectura a través de la independencia entre las capas de identidad, de políticas y de ejecución, la separación de los planos de control y el comportamiento seguro por defecto en condiciones de incertidumbre. Las interrupciones son inevitables. La prioridad es que sigan siendo locales y explicables, y poder resolverlas y utilizarlas para reforzar el sistema. Las organizaciones líderes no son aquellas que no sufren ningún incidente, sino aquellas que logran limitar el alcance de cualquier evento individual.

La contención como ventaja para el crecimiento

Aunque a menudo se considera una garantía, la disociación de las capas favorece la velocidad y el crecimiento. El informe "Cost of a Data Breach Report 2025" de IBM reveló que las organizaciones que utilizan la IA y la automatización redujeron considerablemente los ciclos de vida de las fugas de datos en 80 días, así como el coste promedio de las fugas de datos en 1,9 millones de dólares.[30]

Al restringir el alcance del impacto, los líderes preservan la confianza de los clientes, los reguladores y los inversores, y mantienen la agilidad necesaria para una adopción más segura de la IA, una entrada más rápida en el mercado y menos escaladas ejecutivas. Cuando se contiene el fallo, los líderes mantienen su capacidad de decisión.

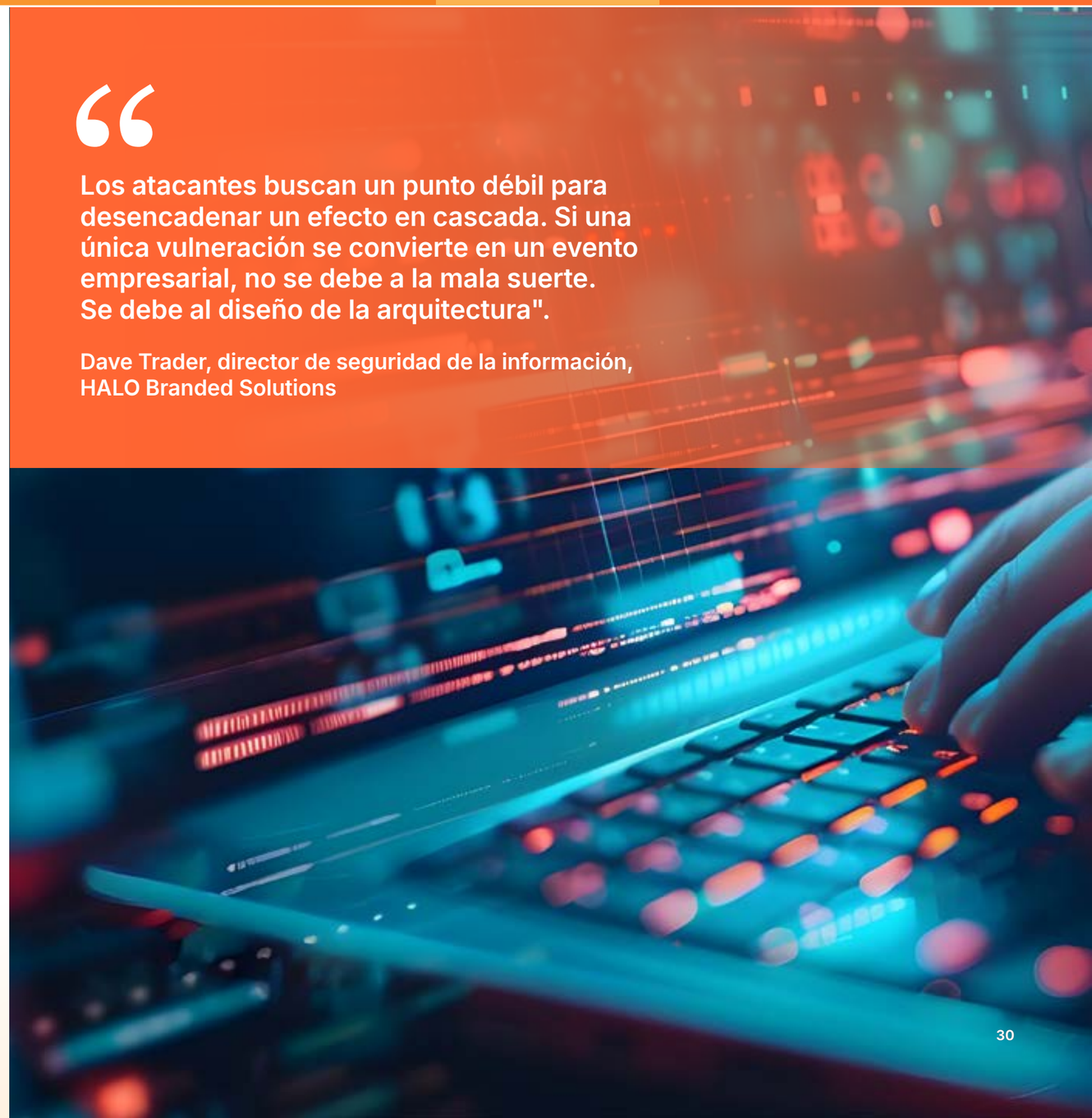
La contención no es defensiva. Permite un movimiento más rápido y una asunción de riesgos más inteligente en un entorno volátil.

Diseñar priorizando los fallos desde la cúpula

A medida que los sistemas digitales sustentan la estrategia empresarial, la decisión de separar o vincular la infraestructura se convierte en una decisión empresarial decisiva.

Los ejecutivos deben pasar de centrarse en la rapidez de la recuperación a considerar qué es lo que nunca puede fallar al mismo tiempo. Eso requiere comprender bien los planos de control compartidos, las dependencias de identidad y las canalizaciones, así como los resultados de las pruebas de modo de fallo, no solo del tiempo de actividad. La contención corresponde al consejo de administración, ya que el fallo sistémico es un riesgo empresarial; no se puede delegar. Debe diseñarse deliberadamente desde la cúpula para que ningún fallo llegue a ser un evento que afecte a toda la empresa, y que cada incidente fortalezca el sistema.

> **“Los atacantes buscan un punto débil para desencadenar un efecto en cascada. Si una única vulneración se convierte en un evento empresarial, no se debe a la mala suerte. Se debe al diseño de la arquitectura".**
>
> **Dave Trader, director de seguridad de la información, HALO Branded Solutions**



PREGUNTAS PARA EL EQUIPO DIRECTIVO

Cuando falla un servicio compartido, ¿la arquitectura lo contiene?

Estas preguntas, debatidas en conjunto, revelan si la empresa puede contener la interrupción en tiempo real, o si la estabilidad sigue dependiendo de la esperanza, el heroísmo y la recuperación posterior a un incidente.

P1

¿Qué sistemas esenciales pueden fallar sin que se detengan las actividades empresariales?

¿Lo hemos demostrado mediante pruebas, o es algo teórico?

→

P2

Si fallara la identidad o una plataforma básica, ¿qué ingresos se bloquearían?

¿Conocemos el impacto de antemano, o solo después de la interrupción?

→

P3

¿La multinube reduce el riesgo o solo aumenta la complejidad y los costes?

¿Dónde hemos reducido la dependencia y dónde sigue estando presente?

→

P4

¿Medimos la contención o solo el tiempo de recuperación?

¿Nuestros KPI incentivan la prevención o la limpieza reactiva?

→

P5

¿Podríamos explicar nuestra última interrupción a la junta o a los reguladores?

¿El impacto ha sido menor gracias al diseño o se debe a una circunstancia afortunada?

CONCLUSIÓN

Los principios de liderazgo para una ventaja duradera

En un mundo determinado por las decisiones basadas en la IA, los sistemas autónomos y los ecosistemas digitales muy interdependientes, la resiliencia ya no es suficiente. La ventaja será gracias a los sistemas que tengan la capacidad de detectar las situaciones difíciles, adaptarse en tiempo real, contener los fallos y seguir funcionando sin esperar la intervención humana. Es lo que llamamos resiliencia autónoma.

Este informe no es un inventario de amenazas. Define el cometido de los equipos directivos: identificar y abordar los desafíos integrados en las empresas modernas. Estas debilidades estructurales pueden parecer controlables en condiciones estables. Sin embargo, si no se toman las medidas decisivas, indudablemente saldrán a la luz en situaciones difíciles. Se propagan con la adopción de la IA, la dependencia de la nube, la arquitectura heredada, la información sobre amenazas y los modelos operativos creados para una era más predecible.

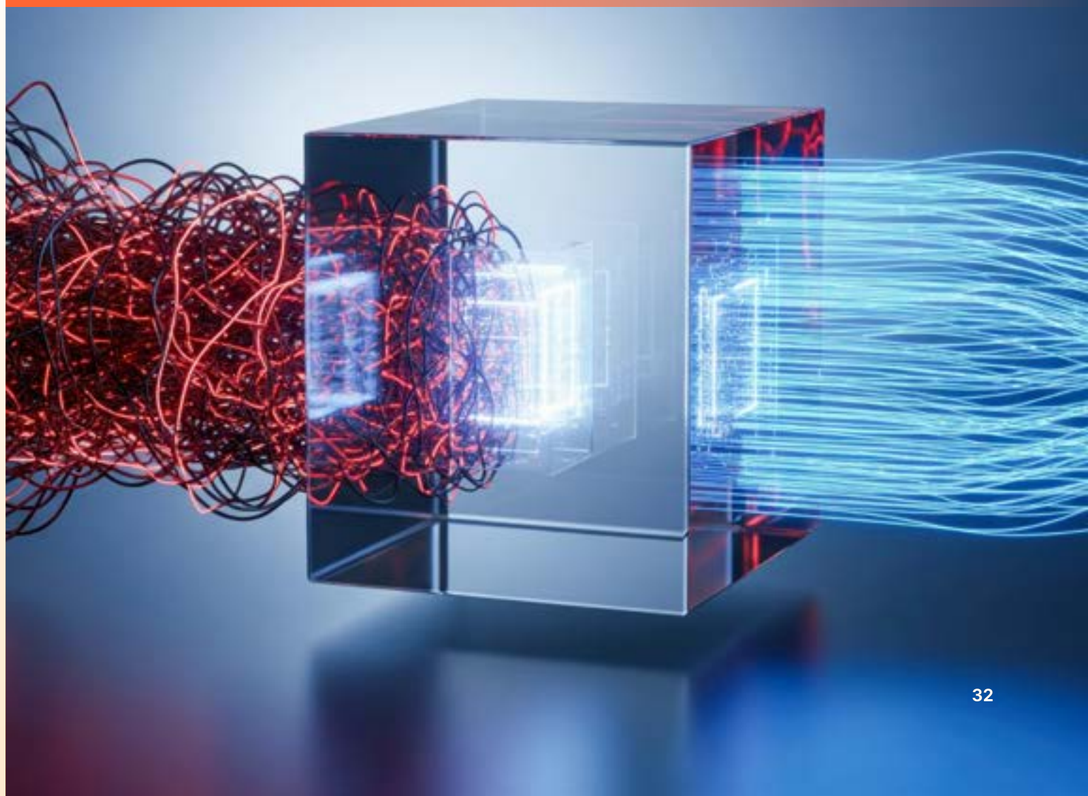
Afrontar estos desafíos no es competencia exclusiva de los CISO. La resiliencia autónoma es una responsabilidad del equipo directivo, determinada por la forma en que los equipos ejecutivos establecen las prioridades, asignan autoridad y diseñan sistemas autoregulables. Las organizaciones autónomas se distinguen por los principios que sus equipos directivos encarnan sistemáticamente:

- **Responsabilidad compartida del riesgo sistémico en lugar de responsabilidad delegada.** El riesgo sistémico es responsabilidad del equipo directivo, no se delega a otros en el organigrama. La responsabilidad es explícita y compartida entre los directivos, y los consejos de administración se involucran en escenarios reales, sopesando las distintas opciones, no mediante informes estáticos.
- **Ejecución inherente a los sistemas en lugar de una intención declarada.** Las decisiones solo importan si se ejecutan a la velocidad de las máquinas. El control sobre los modelos, los datos, las instrucciones y las acciones autónomas debe residir donde se produce la ejecución. Los elementos que dependan de la documentación, la alineación o el proceso manual no se escalarán.
- **Independencia estructural en lugar de la comodidad a corto plazo.** Lo que parece eficiente en condiciones tranquilas a menudo crea fragilidad en situaciones difíciles. Los equipos con resiliencia autónoma priorizan la contención, la reversibilidad y la separación. Los sistemas están diseñados para que los fallos sigan siendo locales, observables y corregibles. La capacidad de evitar un efecto en cascada pasa a ser una ventaja estratégica.
- **Confianza demostrable en lugar de control asumido.** La confianza debe ser siempre demostrable, no implícitamente asumida. Los directivos exigen visibilidad del comportamiento del sistema, controles aplicables a las identidades de los usuarios y de las máquinas, y pruebas de integridad a la velocidad de las máquinas. La confianza asumida falla en un contexto de autonomía.
- **Aprender del fracaso en lugar de evitar el fracaso.** El fallo se espera y se utiliza deliberadamente como una enseñanza. La detección temprana, el alcance limitado, la recuperación rápida y el aprendizaje institucional definen un desempeño de liderazgo. La velocidad de recuperación, no la prevención, es la métrica que importa.

En 2026, el liderazgo se define menos por la planificación para la estabilidad y más por el diseño para hacer frente a las interrupciones.

Las organizaciones líderes serán aquellas cuyos ejecutivos incorporen estos principios en sus decisiones cotidianas, convirtiendo la volatilidad en aprendizaje, las situaciones difíciles en avances y la incertidumbre en una ventaja.

Las organizaciones líderes serán aquellas cuyos ejecutivos incorporen estos principios en sus decisiones cotidianas, **convirtiendo la volatilidad en aprendizaje, las situaciones difíciles en avances y la incertidumbre en una ventaja.**



Acerca de Cloudflare

ACERCA DE CLOUDFLARE

Una plataforma. Una red programable.

Más de 330 ciudades

en más de 125 países, incluida China continental

con más de 210 ciudades

con GPU para inferencia de IA en todo el mundo

~50 ms

de aproximadamente el 95 % de la población mundial conectada a Internet

~13 000 redes

que se conectan directamente a Cloudflare, incluidos proveedores de acceso a Internet, proveedores de nube y grandes empresas

477 Tb/s

de capacidad de red (y continúa creciendo)

ACERCA DE CLOUDFLARE

Suite de seguridad de Cloudflare

Resiliencia y protección perimetral

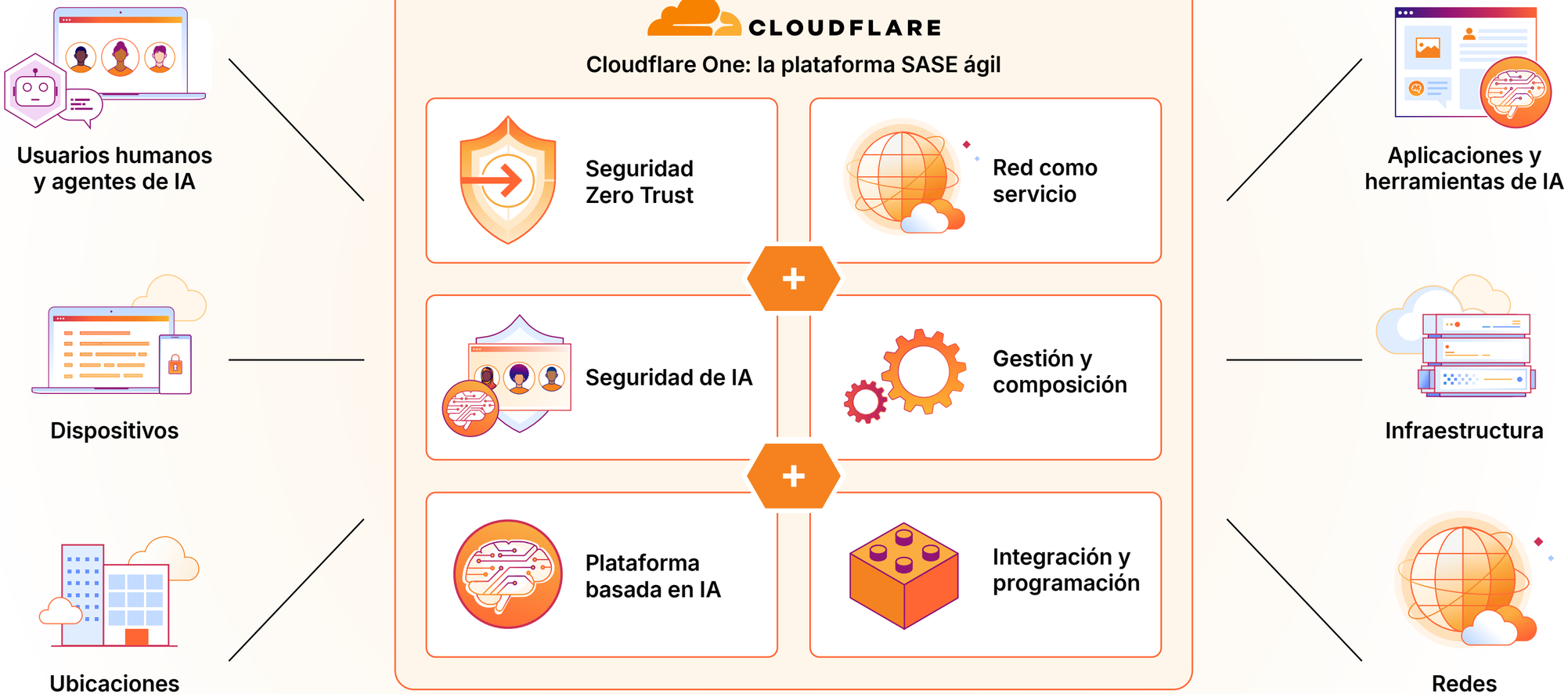
- Protección de aplicaciones web y API: bloquea los ataques, detecta las vulnerabilidades y mejora la disponibilidad.
- Servicio de seguridad en el perímetro (SSE): aplica la seguridad Zero Trust a todos tus equipos de trabajo híbridos.
- Mitigación de DDoS: resiste los ataques más grandes y avanzados con una capacidad de red de 477 Tb/s.

Integración segura de la nube y de la red

- Perímetro de servicio de acceso seguro (SASE): conecta y protege a tus usuarios, tus agentes de IA y tu infraestructura.
- Red como servicio y multinube: conecta, protege y acelera tu red corporativa sin el coste y la complejidad del hardware de red heredado.
- Interconexión de red: conecta directamente tus redes locales y en la nube a la red de Cloudflare.

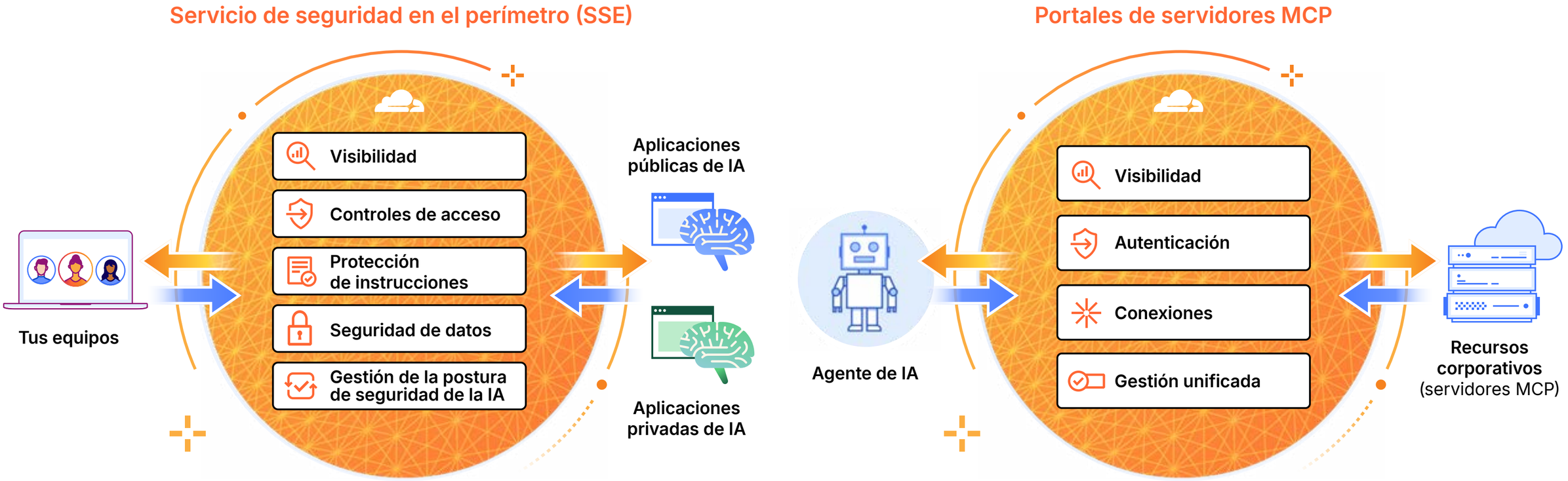
ACERCA DE CLOUDFLARE

Servicios Cloudflare One



ACERCA DE CLOUDFLARE

Protege el uso de la IA generativa y controla los agentes de IA



ACERCA DE CLOUDFLARE

Servicios de IA de Cloudflare durante todo el ciclo de vida

Desarrolla la IA
con la plataforma para desarrolladores

Desarrolla la IA en todas las regiones del mundo con un solo clic

Workers AI, Vectorize, AI Gateway

Crea fácilmente una infraestructura dedicada a la IA

Servidor MCP remoto, SDK de agentes, AI Search, AI Gateway

Protege la adopción de la IA
con AI Security Suite

Protege la utilización de la IA generativa por parte de tus equipos de trabajo

Plataforma SASE (Cloudflare One)

Controla los agentes de IA

Servicios ZTNA de Cloudflare, con los portales de servidores MCP

Desarrolla la IA con total seguridad

AI Gateway

Protege tus aplicaciones de IA

Seguridad de las aplicaciones, con Firewall for AI

Protege tu contenido
con los servicios para aplicaciones

Protege tu contenido original en línea contra los rastreadores de IA

Bot Management, con AI Crawl Control

Plataforma basada en IA en una red global
Modelos de detección de amenazas | Agente de IA (Cloudy) | Modelos de prevención de pérdida de datos

ACERCA DE CLOUDFLARE

Información para los directores ejecutivos modernos

Sortear el panorama actual de las amenazas y los rápidos cambios tecnológicos requiere algo más que conocimientos operativos: exige previsión estratégica. "The Executive Lens" de Cloudflare es un centro de recursos dedicado específicamente a los altos directivos.

Descubre análisis de los expertos, marcos prácticos y estudios exclusivos sobre temas empresariales fundamentales, como la ciberresiliencia, la gobernanza segura de la IA y la transformación digital global.

Lee hoy mismo The Executive Lens.

Más información

Recursos adicionales

Forrester Total Economic Impact

Responde a las amenazas sofisticadas y evita las emergentes. Descubre cómo Cloudflare ayuda a las empresas a utilizar la seguridad como una ventaja competitiva, para hacer frente a un complejo panorama de amenazas con mayor eficiencia y previsibilidad.

Más información

Security Signal

Descubre las señales entre el ruido y céntrate en las tendencias de ciberseguridad más importantes de la actualidad. Cada episodio de Security Signal traduce las complejidades de la ciberseguridad en información práctica para los ejecutivos al mando.

Ver ahora

Informe de Cloudflare sobre amenazas 2026

[Solo en inglés] Te explicamos el panorama de las amenazas para 2026 definido por una nueva medida de eficacia (MOE). El informe detalla los nuevos riesgos derivados del posicionamiento previo financiado por estados, el robo de tokens, los ataques DDoS hipervolumétricos y mucho más.

Más información

theNET

Perspectivas sobre la innovación en ciberseguridad, el panorama de las amenazas y el futuro de Internet con perspectivas ejecutivas sobre cómo resolver los retos organizativos gracias a la tecnología.

Más información

the NET BY CLOUDFLARE

Contactos

	Global	América	Europa, Oriente Medio y África	Asia Pacífico	Japón
Liderazgo en el mercado	 **Mark Anderson** Director de Ingresos markanderson@cloudflare.com	 **Rick Congdon** Vicepresidente, América congdon@cloudflare.com	 **Tony Van den Berge** Vicepresidente, EMEA tonyberg@cloudflare.com	 **Goran Risticevic** Vicepresidente, APAC goran@cloudflare.com	 **Sayoko Matsumoto** Vicepresidente, Japón sayoko@cloudflare.com
Equipo de directores ejecutivos	 **Ramy Houssaini** Director de soluciones de ciberseguridad ramy@cloudflare.com	 **Khalid Kark** Director de informática, América khalid@cloudflare.com	 **Christian Reilly** Director de informática, EMEA creilly@cloudflare.com	 **Volker Rath** CISO volker@cloudflare.com	 **Koichiro Otobe** Director técnico, Japón koichiro@cloudflare.com

CLOUDFLARE

2026

Informe de seguridad Cloudflare Signals

Resiliencia autónoma

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-8897.2026MAR19

Notas finales

1. Jonathan Villa, “Hidden Risks of Shadow AI”, Varonis, www.varonis.com/blog/shadow-ai. Consultado el 11 de febrero de 2026.
2. IBM, “Cost of a Data Breach Report 2025”, www.ibm.com/reports/data-breach. Consultado el 11 de febrero de 2026.
3. MultiState, "Artificial Intelligence (AI) Legislation", www.multistate.ai/artificial-intelligence-ai-legislation. Consultado el 11 de febrero de 2026.
4. Gartner, "Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up From Less Than 5% in 2025", 26 de agosto de 2025, www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025. Consultado el 11 de febrero de 2026.
5. Cloudflare Radar, "Bot Traffic", radar.cloudflare.com/bots?dateRange=12w. Consultado el 11 de febrero de 2026.
6. Cloudflare Radar, "Seguridad de la capa de aplicación", radar.cloudflare.com/security/application-layer?dateRange=12w. Consultado el 11 de febrero de 2026.
7. IBM, "Cost of a Data Breach Report 2025".
8. Lareina Yee, et al., "The AI Reckoning: How Boards Can Evolve", McKinsey & Company, 24 de octubre de 2024, www.mckinsey.com/capabilities/mckinsey-technology/our-insights/the-ai-reckoning-how-boards-can-evolve. Consultado el 11 de febrero de 2026.
9. IBM, "Cost of a Data Breach Report 2025".
10. ENISA, "SBOM Analysis - Towards an Implementation Guide", diciembre de 2025, www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf. Consultado el 11 de febrero de 2026.
11. Verizon, "2025 Data Breach Investigations Report (DBIR)", www.verizon.com/business/resources/reports/dbir. Consultado el 11 de febrero de 2026.
12. Cloudflare, "Informe de Cloudflare sobre innovación en aplicaciones 2026", 2026, www.cloudflare.com/resource/g/app-innovation-report/2026. Consultado el 11 de febrero de 2026.
13. CrowdStrike, "2025 Global threat report", www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf. Consultado el 18 de marzo de 2026.
14. SANS Institute, "SANS 2025 CTI Survey: Cyber Threat Intelligence Survey", SOCRadar, mayo de 2025, socradar.io/wp-content/uploads/2025/05/SANS-2025-CTI-Cyber_Threat_Intelligence_Survey-SOCRadar.pdf. Consultado el 11 de febrero de 2026.
15. SANS Institute.
16. SANS Institute.
17. Mohammed Khalil, "Vulnerabilities Statistics 2025: Record CVEs, Zero-Days & Exploits", DeepStrike, 8 de octubre de 2025, deepstrike.io/blog/vulnerability-statistics-2025. Consultado el 25 de febrero de 2026.
18. VulnCheck, "VulnCheck State of Exploitation 2026", 21 de enero de 2026, www.vulncheck.com/blog/state-of-exploitation-2026. Consultado el 11 de febrero de 2026.
19. Datos de la red global de Cloudflare.
20. Pegasystems, "Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research", 14 de octubre de 2025, www.pega.com/about/news/press-releases/average-global-enterprise-wastes-more-370-million-every-year-through. Consultado el 11 de febrero de 2026.
21. Protiviti, "Global Technology Executive Survey: Tech Debt a Major Burden", www.protiviti.com/us-en/global-technology-executive-survey-tech-debt-major-burden. Consultado el 11 de febrero de 2026.
22. Cloudflare, "Informe de Cloudflare sobre innovación en aplicaciones 2026".
23. Pegasystems, "Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research".
24. Cloudflare, "Informe de Cloudflare sobre innovación en aplicaciones 2026".
25. Cloudflare, "Informe de Cloudflare sobre innovación en aplicaciones 2026".
26. Uptime Institute, "Uptime Annual Outage Analysis Report 2025", 6 de mayo de 2025, uptimeinstitute.com/about-ui/press-releases/uptime-announces-annual-outage-analysis-report-2025. Consultado el 11 de febrero de 2026.
27. Nuno De la Torre, et al., "IT Resilience for the Digital Age", McKinsey & Company, 20 de junio de 2023, www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/it-resilience-for-the-digital-age. Consultado el 11 de febrero de 2026.
28. Ashwin Chaudhary, "Managing Cloud Misconfigurations Risks", Cloud Security Alliance, 14 de agosto de 2023, cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks. Consultado el 11 de febrero de 2026.
29. IBM, "Cost of a Data Breach Report 2025".
30. IBM, "Cost of a Data Breach Report 2025".