CLOUDFLARE

2026

Informe Security Signals de Cloudflare

Resiliencia autónoma

PRÓLOGO DE MICHELLE ZATLYN

Todo está cambiando.

La IA está pasando de la fase piloto a la de producción, los sistemas autónomos están acelerando la toma de decisiones y la economía digital está evolucionando en tiempo real. Para los líderes que están listos para actuar, ese ritmo de cambio crea una oportunidad real.

La resiliencia se ha convertido en la nueva ventaja competitiva. A medida que los sistemas inteligentes transforman la economía digital, los líderes pueden diseñar defensas para anticipar el cambio, crear sistemas que se adapten y convertir la volatilidad en una ventaja.

Cloudflare gestiona 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, detenemos más de 230 mil millones de ciberataques diarios y gestionamos 2500 millones de solicitudes de bots al día. Desde este punto de vista, vemos tanto los riesgos como las oportunidades que configuran Internet.

El ***Informe Security Signals de Cloudflare 2026*** ofrece la información práctica que los líderes necesitan hoy en día, y mapea las fuerzas que están redefiniendo el panorama digital, para que puedas gestionar sistemas inteligentes, modernizar de forma segura y desarrollar la resiliencia desde el núcleo.

Nuestra misión es contribuir a construir un Internet mejor. En 2026, eso significa que puedas trabajar de forma segura y confiable, a la velocidad de una máquina.

Michelle Zatlyn
Cofundadora, presidenta
y copresidenta de Cloudflare

RESUMEN EJECUTIVO

Para las empresas actuales sumamente interconectadas y automatizadas, el modelo de "absorber los impactos y garantizar la recuperación" ya no funciona.

Este enfoque se basa en la suposición ingenua de que podemos predecir con precisión y prepararnos para cada interrupción específica. 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 **resiliencia autónoma: sistemas que no solo resistan el estrés, sino que se regulen, se adapten y se recuperen en tiempo real**.

Sin embargo, aunque muchas organizaciones parecen maduras, modernas y bien administradas, la resiliencia autónoma no es visible en un estado estable. Es un resultado de liderazgo que solo se revela bajo un estrés sostenido y severo.

Este informe se basa en una premisa simple: los mayores riesgos que enfrentarán las empresas en 2026 no provienen de debilidades obvias. Emergen de desafíos ocultos, áreas que parecen sólidas en las operaciones normales, pero que se fracturan cuando aumenta la velocidad, la escala o las interrupciones.

En estos capítulos, ofrecemos a los ejecutivos un plan para detectar desaflíos antes de que colapsen. Cada sección ofrece preguntas específicas para iniciar el debate interno y descubrir la fragilidad oculta dentro de sus propias organizaciones. En una era de inteligencia, autonomía y velocidad, el éxito pertenece a los líderes que diseñan sus empresas para detectar, adaptarse y autocorregirse bajo estrés, mientras protegen los resultados críticos a medida que cambian las condiciones.

Seis desafíos críticos

Estos desafíos no son un caso aislado. La presión en una zona puede intensificar la debilidad en otras.

1 Domar el algoritmo: controlar la IA a gran escala

Los programas de IA suelen parecer disciplinados, regulados y basados en valores. Sin embargo, bajo escrutinio, muchos líderes no pueden explicar claramente dónde se ejecuta la inteligencia artificial, qué datos maneja o quién es responsable cuando los resultados fallan. El progreso en la superficie a menudo oculta una brecha de visibilidad y propiedad que se expone cuando los reguladores, los clientes o los incidentes ejercen presión.

2 Confianza a la velocidad de la máquina: autonomía de ingeniería

Los sistemas autónomos funcionan bien cuando las condiciones son predecibles. Bajo estrés, las decisiones se toman más rápido que la supervisión humana, y la confianza se da por sentada en lugar de construirse. Este desafío prueba si la delegación fue deliberada o si la autoridad cambió discretamente a las máquinas sin límites claros, responsabilidad o control en tiempo real.

3 Cadenas de suministro paralelas: exposición de dependencias ocultas

Las empresas parecen diversificadas y con muchos socios, pero dependen de capas de servicios de terceros y de cuartos que no ven por completo. 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 oculto.

4 Señales de intención: de la inteligencia a la previsión

Si bien los programas de inteligencia basada en datos suelen parecer integrales, la información que llega demasiado tarde no influye en las decisiones. Este desafío a las organizaciones que utilizan señales tempranas para perfeccionar continuamente las decisiones, fortalecer la anticipación y mejorar la capacidad de respuesta con el tiempo, de aquellas que solo aprenden después de que el daño ya está hecho.

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

Las arquitecturas heredadas pueden parecer estables en las operaciones diarias. Bajo la velocidad de los ataques modernos y el escrutinio normativo, se vuelven frágiles y consumen tiempo, talento y resiliencia más rápido de lo que las organizaciones pueden adaptarse. Este desafío expone si la arquitectura permite la evolución o la limita sutilmente.

6 Espejismo en la nube: desacoplamiento del riesgo de cascada

Las estrategias en la nube ofrecen escalabilidad y eficiencia, pero los planos de control compartidos y las dependencias estrictas centralizan los fallos. Cuando llega el estrés, los sistemas se derrumban. Esto prueba si la resiliencia está diseñada para la contención o simplemente se da por sentada a través de planes de recuperación. Las organizaciones maduras limitan el radio de impacto y se vuelven más tolerantes a 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 al que los modelos de marcos de control empresarial no logran adaptarse. 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. Pero antes de que la IA actúe de forma independiente, la visibilidad, la propiedad y las restricciones ya deben estar establecidas. Una vez que las decisiones se toman a la velocidad de la máquina, estas cuestiones ya no se pueden debatir.

Si bien la mayoría de los equipos ejecutivos reconocen que la IA es un asunto de la alta dirección, pocos pueden expresar claramente dónde se utiliza la IA, qué datos maneja o cómo se gestiona el riesgo en toda su empresa. Esta brecha entre el conocimiento y el control de la IA es ahora uno de los puntos ciegos más importantes en el liderazgo moderno.

La pregunta ya no es si la IA ofrece valor. Es si el liderazgo tiene suficiente visibilidad para controlar el impacto de la IA en la resiliencia, la confianza, el costo y la responsabilidad a gran escala.

La IA ya no es experimental. Opera en el corazón de la empresa, y debe regirse con el mismo rigor que el dinero, el riesgo y la regulación. En este entorno, la confianza es el verdadero diferenciador.

La velocidad gana. El permiso pierde.

La accesibilidad de la IA ha cambiado radicalmente la forma en que la tecnología se integra en la organización. Los empleados y los equipos ya no esperan la aprobación centralizada. Las herramientas de IA se adoptan de manera discreta —a través de extensiones de navegador, funciones SaaS integradas, API y plataformas para desarrolladores— a menudo con buenas intenciones y ganancias de productividad inmediatas.

La consecuencia es predecible: la IA se expande a un ritmo más rápido que el de los marcos normativos. De hecho, el 98 % de los empleados utilizan aplicaciones no autorizadas en los casos de uso de la Shadow AI y Shadow IT.[1]

Las herramientas no autorizadas introducen controles de seguridad inconsistentes y prácticas de manejo de datos poco claras, y difuminan la responsabilidad. Para los directorios, esto crea una realidad incómoda. El riesgo de la IA es importante, pero a menudo tiene una medición imprecisa y carece de liderazgo.

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

El marco de control ya no puede ser un paso de validación. Debe convertirse en un sistema siempre activo basado en medidas de seguridad, visibilidad continua y estándares que escalen tan rápido como lo hace la adopción de la IA.

Los datos son el premio y la responsabilidad

Los sistemas de IA obtienen su potencial de la capacidad de acceso: a los datos, a los modelos y a las decisiones posteriores. Bajo la presión de ofrecer resultados rápidos, las organizaciones suelen ampliar el acceso más rápidamente 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 reportaron un incidente de seguridad relacionado con la IA en 2025 carecían de controles de acceso adecuados a la IA.[2]

Los marcos de seguridad tradicionales no se diseñaron para capturar los riesgos nativos de la IA, como la manipulación de prompts, la retención de datos no intencionada o el uso indebido de modelos. Como resultado, muchas organizaciones pueden certificar el cumplimiento normativo sin comprender realmente la exposición impulsada por la IA.

Los marcos como NIST AI RMF e ISO/IEC 42001 brindan orientación, pero la garantía real proviene de cómo se implementan y se aplican. Cada sistema de IA es un sistema de datos antes de ser un sistema de inteligencia. Si los líderes no pueden mapear sus flujos de datos, rutas de uso indebido y modos de falla, no están preparados para escalar.

> “Un patrón se repite cada vez que se automatiza la toma de decisiones: los resultados se mueven más rápido que la rendición de cuentas. La IA no crea esa brecha, la expone. Cuando la responsabilidad no está clara, **el marco de control se vuelve performativo**, sin importar lo pulcra que parezca la política.”
>
> Joe Sullivan, ex director de seguridad (CSO), Uber

Shadow AI es Shadow IT con la velocidad de la máquina

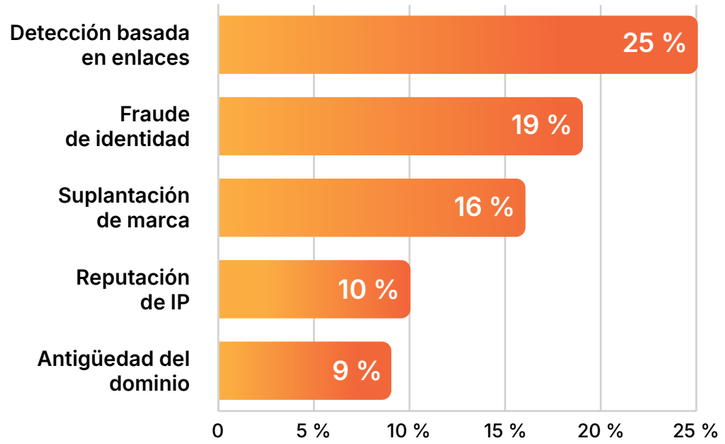
La IA puede proliferar de forma invisible entre empleados, contratistas, equipos de productos y proveedores externos sin activar una revisión formal. Esto crea una brecha de auditabilidad precisamente en el momento en que los reguladores exigen una mayor transparencia.

Los gobiernos y los reguladores exigen cada vez más inventarios de IA documentados, linaje de datos rastreable y explicabilidad para las decisiones automatizadas. La incapacidad para demostrar el control se está convirtiendo rápidamente en una falla de cumplimiento normativo, no solo en un problema de madurez.

Las organizaciones líderes que están subsanando esta brecha están pasando de las auditorías episódicas 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 inteligencia artificial (IA) no se puede registrar, explicar y evidenciar, no se puede defender ante los reguladores, los clientes o la junta.

Principales categorías de amenazas en la detección de correos electrónicos



Nota: los porcentajes no suman el 100 %, ya que los correos electrónicos pueden tener varias categorías de amenazas.

Fuente: Cloudflare Radar

Los ataques basados en enlaces y el fraude de identidad dominan las amenazas modernas del correo electrónico. Estas campañas explotan las señales de confianza en lugar de las vulnerabilidades técnicas. A medida que la IA reduce el costo de producir engaños convincentes y personalizados, el marco de control debe ir más allá de la supervisión del modelo para abarcar la autenticación, la integridad de la identidad y la trazabilidad de las decisiones.

> El marco de control suele parecer suficiente **hasta que ocurre algo inesperado**. Con la IA, ese momento llega antes y tiene un impacto más amplio. Las organizaciones que gestionan este cambio con éxito no ven a la IA como una simple herramienta, sino como una cadena de suministro, rastreando el origen, la propiedad y la influencia, incluso cuando se encuentra fuera de sus muros".
>
> Kate Kuehn, directora global de estrategia de ciberseguridad, World Wide Technology

La regulación reside en el código, no solo en la política.

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

Esto indica un cambio más amplio: la gestión de la IA se está replanteando como una responsabilidad empresarial de riesgo y liderazgo, y no como una política técnica discrecional. Las organizaciones que diseñan la gestión de la IA como infraestructura convierten la confianza en un factor de crecimiento, no en una limitación.

> Estamos siendo testigos de la mayor expansión de Shadow IT de la historia, a medida que los empleados adoptan servicios y agentes de IA fuera del marco de control. A diferencia de la Shadow IT tradicional de SaaS, estas capacidades de IA son difíciles de detectar o bloquear; pueden asumir identidades de usuarios reales, integrarse en la actividad estándar y funcionar a la velocidad de una máquina. El mandato del CISO no es bloquear esta adopción, sino diseñar capacidades de IA seguras que eliminen la necesidad de herramientas fuera del marco de control".
>
> Michael Goodman, vicepresidente/director de soluciones digitales y de seguridad (CD y SO), Hitachi

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Revelar los puntos ciegos en la gestión de la IA

A la velocidad de la máquina, la propiedad poco clara, la visibilidad limitada y las medidas de seguridad débiles se convierten en responsabilidades empresariales, por lo que estas preguntas son imperativas para los directivos.

P1

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

¿Y dónde empieza y acaba esa autoridad? ¿Se pone en práctica esta responsabilidad o se asume hasta que algo sale mal?

P2

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

¿Esas limitaciones están definidas claramente, son explícitas, se pueden aplicar y son uniformes entre los equipos, o dependen en gran medida de la confianza de nuestra fuerza laboral en el cumplimiento de 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 con la normativa, pero no están alineados con la intención comercial, la ética o la tolerancia al riesgo? ¿Controlamos los resultados, o solo el acceso y las herramientas? ¿Cómo identificamos las empresas que cumplen y las que no cumplen?

P4

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

¿O las definiciones, el uso de la sombra y la exposición a terceros mostrarían faltantes en nuestro conocimiento?

P5

A medida que se acelera la adopción de la IA, ¿sigue siendo coherente nuestro modelo de marco de control?

¿O se divide entre funciones, proveedores y regiones? ¿El marco de control se considera como un marco estático o como un sistema operativo vivo?

2

Confianza a la velocidad de la máquina: Autonomía de ingeniería

Confianza a la velocidad de la máquina: Autonomía de ingeniería

Las empresas inician su transformación más importante desde la Internet comercial. Hemos pasado de las herramientas asistidas por IA a la era de la "empresa autónoma", en la que los agentes de IA y los flujos de trabajo de agentes ejecutan procesos empresariales de extremo a extremo con una intervención humana mínima o nula. Esta línea de falla asume que los sistemas de IA ya están integrados y actúan de manera autónoma. A diferencia del desafío de gestión de la IA, que se centra en la visibilidad, la supervisión y la responsabilidad, esta línea de falla aborda lo que sucede después de que la autoridad ya se ha delegado a las máquinas. La pregunta ya no es dónde se utiliza la IA o a quién pertenece; es si la confianza se mantiene cuando las decisiones se toman sin la presencia de humanos.

Gartner predice que para 2026, se espera que casi la mitad de las aplicaciones empresariales integren agentes de IA para tareas específicas, en comparación con la adopción de un solo dígito solo un año antes.[4] Este cambio ofrece una velocidad y eficiencia sin precedentes, al mismo tiempo que introduce un riesgo estructural: las decisiones empresariales ahora superan 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 la máquina. Asegurar este futuro requiere un cambio fundamental, de "confiar pero verificar" a "confianza por diseño" y, en última instancia, a sistemas que se vuelvan más confiables a medida que se prueban.

La "paradoja de la velocidad": cuando el negocio se mueve más rápido que la supervisión

La seguridad tradicional requiere tiempo. Se genera una alerta. Un humano investiga. Se toma una decisión. Los sistemas autónomos eliminan esa ventana. 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, el impacto se produce antes de que un humano pueda intervenir.

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

La implicación es clara: la seguridad no puede quedarse fuera del sistema. Debe estar integrado en la propia capa de decisión, que rija la intención, no solo el acceso. Esta línea de falla no se trata de predecir ataques. Se trata de garantizar que cuando sus propios sistemas actúen, lo hagan dentro de los límites diseñados deliberadamente por el liderazgo.

El nuevo plano de control para la IA autónoma

1. La identidad debe ir más allá de los humanos

Las identidades no humanas, agentes de IA, cuentas de servicio, bots, ahora superan en número a los usuarios humanos por órdenes de magnitud. Los bots son responsables de aproximadamente el 30 % del tráfico HTTP que Cloudflare sirve,[5] y un asombroso 92 % de todos los intentos de inicio de sesión observados por Cloudflare provienen de bots, a menudo ataques de relleno de credenciales.[6] Sin embargo, la mayoría de las empresas siguen gestionando 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 limitada o controles de ciclo de vida. Cuando están comprometidos, operan con un radio de acción masivo.

Cada agente de IA debe tener una identidad criptográfica verificable, administrada a través de la gestión de identidad de la máquina. Las credenciales deben ser de corta duración, sensibles al contexto y revocables en tiempo real. La autonomía sin identidad es una renuncia.

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

Fuente: Cloudflare Radar

Ya no operamos en una Internet que prioriza a los humanos. Los algoritmos interactúan cada vez más entre sí, a menudo sin supervisión humana directa. Los modelos de marco de control basados en la autenticación de usuarios y los controles de acceso de los empleados no están alineados con esta realidad.

2. Los sistemas probabilísticos requieren medidas de seguridad deterministas

Los sistemas de IA operan mediante razonamiento probabilístico. La seguridad no puede fallar. Si bien los agentes pueden optimizar, negociar o recomendar, las reglas que rigen lo que se les permite hacer deben ser de carácter absoluto. Las políticas no se pueden inferir, se deben aplicar.

Esto requiere:

- Política como código que define restricciones no negociables
- Capas de cumplimiento en tiempo real que interceptan la intención antes de la ejecución
- Separación entre la toma de decisiones y la autorización

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

> El juicio humano sigue siendo esencial, pero ya no funciona a la velocidad que requieren los sistemas. En entornos en los que las máquinas interactúan continuamente, **la confianza debe asumirse, imponerse y verificarse desde el 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, la seguridad de ayer se vuelve rápidamente irrelevante. Sin una observabilidad profunda, los líderes no pueden distinguir entre el comportamiento autónomo legítimo y la manipulación.

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

El argumento económico

La integración de la IA y la automatización en las operaciones de seguridad ofrece beneficios financieros medibles. Las organizaciones que utilizan estas funciones de manera generalizada resuelven las brechas 80 días más rápido y reducen los costos promedio de las brechas en USD 1,9 millones en comparación con las que no lo hacen.[7]

La ventaja va más allá de la reducción de costos. Con medidas de seguridad sólidas, los directivos adquieren la confianza necesaria para implementar la automatización en los flujos de trabajo esenciales para los ingresos, lo que mejora la capacidad de respuesta, la velocidad del capital y la diferenciación competitiva. Una autonomía bien gestionada se convierte en un factor de crecimiento, y no solo en un control de riesgos. La seguridad a la velocidad de la máquina no es una sobrecarga. Es el precio de escalar la autonomía sin fragilidad.

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 todos los ejecutivos de alto nivel (C-suite). El liderazgo en seguridad ya no se trata de proteger los sistemas después de que se toman las decisiones, se trata de orquestar la confianza en entornos donde las máquinas actúan de forma independiente.

Un CISO recordó la primera vez que un sistema de IA detuvo una transacción multimillonaria por sí solo. La decisión fue correcta, pero generó una pregunta más profunda en la sala de juntas: ¿Quién había autorizado realmente a la máquina a hacer esa llamada? La tecnología se adelantó al marco de control.

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

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

A medida que se extiende la autonomía, la seguridad, el cumplimiento normativo y la tecnología ya no pueden operar en silos. La seguridad influye en la velocidad de los ingresos. El cumplimiento normativo determina el acceso al mercado. La tecnología define la responsabilidad. La confianza a la velocidad de la máquina no es un programa de seguridad, es un sistema de liderazgo que unifica la resiliencia, el marco de control, la innovación y la reputación bajo un mandato ejecutivo.

> La automatización cambia la velocidad de las decisiones, pero también cambia el radio de acción de los errores. La pregunta que se hacen los líderes es: "¿Cómo diseñamos 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 ponen de manifiesto si los directivos han diseñado límites intencionadamente en torno a cómo se toman las decisiones a la velocidad de la máquina y cómo se asume el riesgo en tiempo real.

P1

¿Qué decisiones empresariales ya están tomando los sistemas autónomos?

¿Qué decisiones reservamos deliberadamente para los humanos? Ese límite, ¿está diseñado, documentado y revisado, o 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 propiedad del riesgo autónomo está claramente definida mientras el sistema está funcionando, o solo se examina después de que algo sale mal?

P3

¿Dónde las decisiones son ejecutadas por el software y no por las personas?

¿En qué aspectos hemos relajado los controles sobre el software? ¿Se exige a las máquinas estándares más altos que a los humanos o se confía más discretamente en ellas?

P4

¿Podemos explicar y justificar una acción autónoma a medida que ocurre?

¿O se hace días después, durante las revisiones de incidentes? ¿Se puede observar la intención a velocidad de máquina o se reconstruye bajo presión?

P5

¿Nuestro modelo de confianza escala a la velocidad de la máquina?

Si la autonomía se duplicara en el próximo año, ¿absorbería nuestro modelo de confianza la aceleración o fracasaría? ¿La confianza está diseñada para escalar y acelerar o se hereda del marco de control de la era humana?

3

Cadenas de suministro ocultas: Exposición de dependencias ocultas

Cadenas de suministro ocultas: Exposición de dependencias ocultas

Nuestra economía hiperconectada ya no se define por lo que controlas, sino por lo que puede afectarte y que ni siquiera ves. Muchos líderes han reforzado su perímetro, modernizado la infraestructura y reforzado el marco de control, pero los riesgos más importantes ahora están más allá de su línea de visión, integrados en ecosistemas de terceros, cuartos y enésimos de los que no son propietarios ni en los que no pueden influir plenamente. La incómoda verdad: se puede ser operativamente maduro y aún así sistémicamente frágil.

Las cadenas de suministro paralelas no son casos extremos; son el resultado natural del ensamblaje digital a gran escala. Cada integración SaaS, llamada API, biblioteca de código abierto y servicio de IA añade otra capa de riesgo heredado. La pregunta de liderazgo ya no es "¿Tenemos riesgos en la cadena de suministro?" sino "¿Entendemos qué falla externa podría detener los ingresos, erosionar la confianza o desencadenar el escrutinio regulatorio mañana?"

El impacto ya es material. Las fugas en la cadena de suministro promedian USD 4,91 millones, cifra superior a la media global de fugas de USD 4,44 millones.[9] La elección estratégica para los líderes es tratar el riesgo de la cadena de suministro como un ejercicio de cumplimiento normativo y aceptar sorpresas periódicas, o tratarlo como una exposición operativa en vivo que exige visibilidad continua, garantía de tiempo de ejecución y medidas de seguridad arquitectónicas.

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 IA, los componentes de código abierto y las capas de infraestructura subcontratadas que operan mucho más allá de la línea de visión de compras. Las fallas en cualquier lugar de esta red extendida, ya sea una fuga, una interrupción o una falla en el cumplimiento normativo, pueden desencadenar rápidamente en daños al cliente, exposición regulatoria e interrupción sistémica.

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

Cuando los sistemas se ensamblan, en lugar de construirse

Un automóvil moderno lo fabrican cientos de proveedores, y las piezas de hardware, los chips y el software provienen de muchos vendedores, cada uno con sus propias cadenas de suministro. Un pequeño defecto oculto puede convertirse en un problema de seguridad a velocidad de autopista, por lo que los fabricantes de automóviles invierten mucho en trazabilidad y pruebas continuas.

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

La diferencia es la disciplina. En el sector automotriz, se hace un seguimiento de las piezas y las retiradas son precisas. En TI, cuando una biblioteca o un componente de IA se ve comprometido, muchas organizaciones primero buscan saber si están expuestas. Los cuestionarios anuales no pueden seguir el ritmo de los sistemas que cambian semanalmente. La visibilidad y la garantía continua se están volviendo tan esenciales para los sistemas digitales como el control de calidad para los automóviles.

Tres fuerzas están acelerando este riesgo:

- **La confianza por proxy se ha convertido en el modelo operativo predeterminado.** Las empresas confían en sus vendedores. Los vendedores confían en sus proveedores. Pocas partes verifican toda la cadena. Las preocupaciones por la competencia y la visibilidad interna limitada hacen que las subcadenas de suministro rara vez se divulguen 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 datos confidenciales a modelos de terceros. Los equipos de riesgo de terceros a menudo no tienen claro cómo estos modelos utilizan los datos, retienen la información o capacitan sobre los aportes empresariales, lo que aumenta los riesgos normativos, de IP y de soberanía de datos.
- **Las expectativas normativas se están endureciendo.** En todo el mundo, los reguladores están pasando con decisión de la orientación a la aplicación. Se espera cada vez más que las organizaciones demuestren visibilidad de las dependencias de terceros y de cuartos, en particular cuando se trata de datos personales o financieros o de infraestructuras críticas. En el futuro, se espera que los líderes no solo evalúen el riesgo de los proveedores, sino que también cuantifiquen el riesgo operativo derivado de las cadenas de suministro extendidas. ¿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 de identidad observados por Cloudflare Email Security

Las marcas más suplantadas no son objetivos aleatorios. Son plataformas fundamentales 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 la infraestructura digital confiable en un vector de ataque. Las cadenas de suministro paralelas no son solo un riesgo operativo, sino también un riesgo para la identidad y la marca.

De la seguridad estática a la transparencia continua

Resolver el problema de la cadena de suministro paralela no requiere más papeleo. Requiere un modelo operativo diferente. El futuro de la garantía de la cadena de suministro es la transparencia continua: visibilidad en tiempo real de lo que realmente se está ejecutando, conectando e intercambiando datos en todo el ecosistema.

Un CISO describió que no descubrió a un proveedor crítico hasta que apareció tráfico inusual en los registros de red. El proveedor era legítimo, pero nadie se dio cuenta de cuán profundamente estaba integrado. La lección era simple: no se puede gestionar lo que no se ve.

Este cambio ya está en marcha. Las listas de materiales de software (SBOM) y el intercambio de explotabilidad de vulnerabilidades (VEX) están pasando de ser artefactos de cumplimiento normativo a señales operativas. Es de esperar que la adquisición requiera cada vez más no solo contratos, sino también divulgaciones en vivo y legibles por máquina que mapeen los componentes, las dependencias y la explotabilidad a medida que cambian.[10]

Al mismo tiempo, la aplicación se está acercando a los lugares donde se manifiesta el riesgo. Los controles de la capa de red y conectividad permiten a las organizaciones observar el comportamiento, detectar flujos de datos no autorizados e identificar proveedores paralelos a medida que se produce la actividad.

La garantía de la cadena de suministro se convierte en una capacidad operativa en lugar de una revisión periódica. La confianza se verifica continuamente. El riesgo se detecta pronto. El marco de control avanza a la par del ecosistema que intenta proteger.

Confiar, pero verificar continuamente

El 30 % de las brechas en 2025 estuvieron relacionadas con la participación de terceros, el doble que el año anterior[11] , lo que ilustra cómo las relaciones de la cadena de suministro ahora influyen profundamente en la exposición al riesgo más allá de los límites internos tradicionales.

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

La recompensa es tangible. 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 ataques de su cadena de suministro y mejorar la velocidad operativa.[12] No se trata de ajustes técnicos; son elecciones de liderazgo sobre cuánta incertidumbre está dispuesta a tolerar una organización en los sistemas de los que depende todos los días.

> El riesgo rara vez proviene de las dependencias que todos esperan, **sino de las que nadie puede ver**. Cuando la visibilidad es incompleta, las auditorías ofrecen comodidad, pero poca protección. La verdadera resiliencia proviene de arquitecturas que revelan sus dependencias mientras operan".
>
> Tim Brown, CISO, SolarWinds

> **Los ecosistemas interconectados recompensan la velocidad y la especialización, pero también distribuyen el riesgo de una manera que los contratos no pueden capturar. La información operativa, no el papeleo, es lo que en última instancia contiene la exposición".**
>
> **Sandip Wadje, director global de riesgos operativos e inteligencia de tecnologías emergentes, BNP Paribas**

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Controlar el riesgo que no controlas

El riesgo de la cadena de suministro ya no se puede gestionar. Es algo con lo que las organizaciones viven. Decide si ese riesgo es visible y controlado, o débil y asumido.

P1

¿Qué procesos empresariales críticos detendríamos si fallara una dependencia clave?

¿Sabríamos por qué falló? ¿Podemos rastrear los ingresos y el impacto en los clientes hasta dependencias específicas en tiempo real, o solo descubriríamos la exposición cuando el daño ya está hecho?

P2

¿Cómo responderemos a las preguntas normativas o de la junta sobre el riesgo del ecosistema?

¿Podemos responder preguntas sobre estos riesgos sin mencionar un contrato? ¿Tenemos visibilidad técnica sobre la ruta operativa del riesgo de los proveedores?

P3

¿En qué aspectos hemos reducido la visibilidad en la cadena de suministro para preservar la velocidad, la comodidad o las relaciones con los proveedores?

¿Son elecciones deliberadas? ¿Quién decidió aceptar esas compensaciones? ¿Qué dependencias están efectivamente "fuera de los límites" del escrutinio?

P4

¿Con qué rapidez podemos determinar si una vulnerabilidad recién revelada nos afecta?

¿Está claramente asignada la responsabilidad de la respuesta? ¿El descubrimiento de la exposición se mide en minutos, días o semanas?

P5

¿Estamos gestionando el riesgo de la cadena de suministro como una disciplina continua o como una auditoría periódica?

¿Nuestro modelo evoluciona tan rápido como nuestro ecosistema, o simplemente nos confirma que se revisaron los controles del año pasado?

4

Señales de intención: De la inteligencia a la previsión

Señales de intención: De la inteligencia a la previsión

Un vistazo a los titulares te dirá que las actividades de los ciberdelincuentes siguen proliferando, a una velocidad y escala cada vez mayores. Con el reconocimiento asistido por IA y los conjuntos de herramientas, más ciberdelincuentes son capaces de realizar ataques más grandes y más sofisticados que nunca. Además, la ventana entre la aparición de la amenaza y el impacto en el negocio es cada vez más corta, ya que el tiempo promedio que tarda un atacante en comenzar a moverse lateralmente se ha reducido a solo 48 minutos.[13]

La información sobre amenazas, que antes se consideraba una capacidad discrecional, se ha convertido en algo fundamental. El 52 % de las organizaciones cuentan ahora con equipos internos dedicados a la información sobre amenazas (CTI).[14] En el panorama de amenazas en constante cambio, la inteligencia 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 CTI en un contexto empresarial, descifrando las señales del ruido y traduciendo el conocimiento en una previsión práctica.

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

De información táctica a señal estratégica

Las amenazas modernas son de alta velocidad, de gran volumen y cada vez más determinadas por la geopolítica, los incentivos económicos y las vulnerabilidades específicas de la industria. En este entorno, la información sobre amenazas ya no puede tratarse como una función de seguridad opcional o limitarse a revisiones de casillas de verificación de fuentes externas genéricas. El contexto, a nivel empresarial, sectorial y global, es importante, y los ejecutivos deben exigir información que conecte directamente la actividad de las amenazas con el impacto en el negocio, la exposición operativa y el riesgo estratégico.

Claramente, hay demasiada actividad en el frente del atacante para estar al tanto de todo. La defensa requiere velocidad y habilidad, y con frecuencia ambas cosas escasean. Si bien tu estrategia de seguridad debe abordar y reconocer el inventario completo de activos y pasivos bajo tu protección, el uso de la inteligencia para comprender no solo los elementos técnicos de las amenazas, sino también su contexto, te permite ajustar tu programa de seguridad para priorizar la reducción de riesgos en las áreas más importantes para tu organización.

Decidir qué es importante para la organización suele implicar la alineación de la junta directiva y la gerencia sobre cómo integrar los principios empresariales básicos, las fuerzas del mercado, las reglamentaciones y las aportaciones de las partes interesadas. Este contexto es invaluable al evaluar la información sobre amenazas, ya que brinda el contexto necesario para que la empresa determine qué datos de CTI son más útiles.

De esta manera, la información sobre amenazas se puede utilizar para "desconectar" la información superflua, vulnerabilidades irrelevantes o grupos de atacantes que se dirigen específicamente a industrias diferentes, para que puedas concentrar tus recursos donde puedan tener el mayor impacto en función del panorama de amenazas específicas de tu organización. La información sobre amenazas que no influye en las decisiones ejecutivas es simplemente ruido que debe ignorarse.

Principales industrias objetivo de ataques DDoS, 2025

Clasificación	Industria
1	Apuestas y videojuegos
2	Telecomunicaciones
3	Tecnología y servicios
4	Servicios bancarios y financieros
5	Minorista

Esta clasificación es un promedio de los ataques DDoS observados a nivel global tanto en la capa de red como en la de aplicación. La tecnología y los servicios ocupa el primer lugar en ataques a la capa de red. Los juegos y las apuestas ocupan el primer lugar en cuanto a ataques a la Capa de aplicación.

Fuente: Cloudflare Radar

La actividad de los ataques no se distribuye de manera uniforme. Los adversarios priorizan los sectores vinculados al apalancamiento económico, la estabilidad de la infraestructura y la relevancia geopolítica. La concentración en industrias específicas refleja la intención estratégica, no la aleatoriedad. La inteligencia efectiva anticipa dónde se intensificará la presión y alinea las defensas en consecuencia.

La información sobre amenazas ya no es negociable

A medida que la información sobre amenazas evoluciona, su enfoque está cambiando de los indicadores técnicos a la relevancia comercial. Los ejecutivos ahora lo consultan para aclarar qué amenazas son realmente importantes, cómo los cambios geopolíticos y de la industria alteran la exposición, y dónde existe fragilidad en las operaciones, los socios y las personas. La cuestión ya no es si invertir en información sobre amenazas, sino qué tipo de información prioriza y por la que paga la organización.

Para enmarcar las conversaciones presupuestarias, considera dónde CTI ofrece 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 una respuesta reactiva a los incidentes una vez que se producen

Para el director financiero, la información sobre amenazas no se justifica por el volumen de alertas, sino por su capacidad para reducir la probabilidad y el impacto de una interrupción importante del negocio: tiempo de inactividad, fraude, intervención regulatoria o daño a la reputación. Desde el punto de vista organizativo, esto exige claridad. Los acuerdos ad hoc y las funciones de inteligencia con recursos insuficientes no pueden ofrecer información de nivel ejecutivo, ni los resultados que permiten.

Ya sea que se proporcione a través de un equipo interno, socios de confianza o un modelo híbrido, el mandato es el mismo: la información debe ser oportuna, contextual y relevante para la toma de decisiones. La inteligencia que solo explica lo que ocurrió ayer no protege 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 sucedió; la intención explica lo que viene a continuación. La información más valiosa conecta el comportamiento, el contexto y el motivo, **convirtiendo las señales aisladas en previsiones** sobre las que los líderes pueden actuar antes de que se produzcan daños".
>
> Menny Barzilay, cofundador y director general, Percepto

Cómo abordar el panorama de amenazas de 2026

Varias de las fallas analizadas 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 a centrarse en los riesgos que requieren acción, no solo conocimiento.

Utiliza una lente simple: esfuerzo del atacante versus impacto. Las amenazas más importantes son aquellas que crean un impacto empresarial descomunal con un esfuerzo mínimo. En 2026, esto aparece en tres patrones:

- **La industrialización de los ataques:** El cambio de los ataques manuales a la escala automatizada y sin fricciones en la propia infraestructura de nube de una organización
- **Intrusiones que priorizan la identidad:** la transición del ransomware a un evento de inicio de sesión en lugar de un robo
- **Conectividad de la cadena de suministro:** La militarización del tejido conectivo entre los entornos SaaS y API-first

Obtener el ***Informe sobre amenazas de Cloudflare 2026***.

Descargar el informe

El ingrediente que falta: modelado de amenazas

Si bien la integración de la información sobre amenazas en tu práctica de seguridad permite la optimización en todos los aspectos de tu práctica, la estrecha integración con el modelado de amenazas la lleva un paso más allá en el ámbito de un controlador estratégico empresarial.

Aunque cada vez más organizaciones tienen en cuenta el riesgo en la toma de decisiones e incluyen la reducción de riesgos 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 ofrece una taxonomía común que alinea al CISO, al equipo directivo y a la junta en torno a supuestos de riesgo compartidos. Obliga a la claridad en la priorización de activos, la probabilidad de riesgo y el impacto en el negocio si fallan los controles.

La perspectiva obtenida en los ejercicios de modelado de amenazas es intencionalmente de alto nivel; los consejos de administración buscan claridad sobre el riesgo sistémico, las tendencias de amenazas emergentes y si la organización se encuentra en el lado correcto de la división de 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, en combinación con el análisis de información sobre amenazas, proporcionan cálculos de riesgo residual.

La inyección de datos de CTI en el proceso de modelado de amenazas permite un mayor ajuste, proporcionando una base para actividades como la validación de controles y la detección de amenazas, ambos elementos esenciales en una postura de seguridad proactiva. Además, la información relevante para el sector puede confirmar si las defensas están reforzadas contra los adversarios más probables, y ofrecer a los responsables de la toma de decisiones indicadores sólidos para la planificación presupuestaria y estratégica.

Sin modelado de amenazas, la inteligencia se mantiene operativa. Con ella, la inteligencia se vuelve estratégica.

> La buena inteligencia reduce el ruido. Una gran inteligencia cambia las decisiones. La diferencia es si ayuda a los líderes a anticipar los movimientos, no solo a explicarlos".
>
> Troy Wilkinson, asesor de riesgo, YL Ventures

Solo 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, cuando se gestiona adecuadamente, conecta la seguridad, el riesgo, las operaciones, las finanzas y la estrategia en una visión ejecutiva consistente de la exposición y la intención.

P1

¿Estamos protegiendo lo que es familiar o lo que es más importante?

¿Hemos alineado explícitamente nuestras defensas con las amenazas que podrían interrumpir los ingresos, las operaciones o la confianza este año?

→

P2

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

¿En qué casos estamos descubriendo ataques a partir del daño causado en lugar de la inteligencia? ¿Estamos a la vanguardia del ciclo de amenazas o a la zaga?

→

P3

¿Los informes sobre amenazas impulsan las decisiones o solo comparten información?

¿Esta información cambia las prioridades, la inversión o el apetito de riesgo en tiempo real?

→

P4

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

¿Hemos diseñado flujos de trabajo asumiendo que el juicio humano puede ser manipulado o suplantado?

→

P5

¿Con qué rapidez podemos recalibrar cuando los adversarios cambian sus estrategias?

¿Qué mecanismos existen para indicarnos 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. En 2025, las organizaciones ya estaban al límite de la capacidad de gestionar más de 130 vulnerabilidades nuevas cada día, casi el 40 % de las cuales se calificaron como altas o críticas.[17] A medida que la IA utilizada como arma vuelve indefendibles las arquitecturas heredadas, 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 ataques expuesta, que agrava el riesgo más rápido de lo que los equipos humanos pueden responder. Aquellos que se modernicen con decisión no solo reducirán el riesgo, sino que también obtendrán la velocidad, la confianza y la adaptabilidad necesarias para competir en la economía impulsada por la IA.

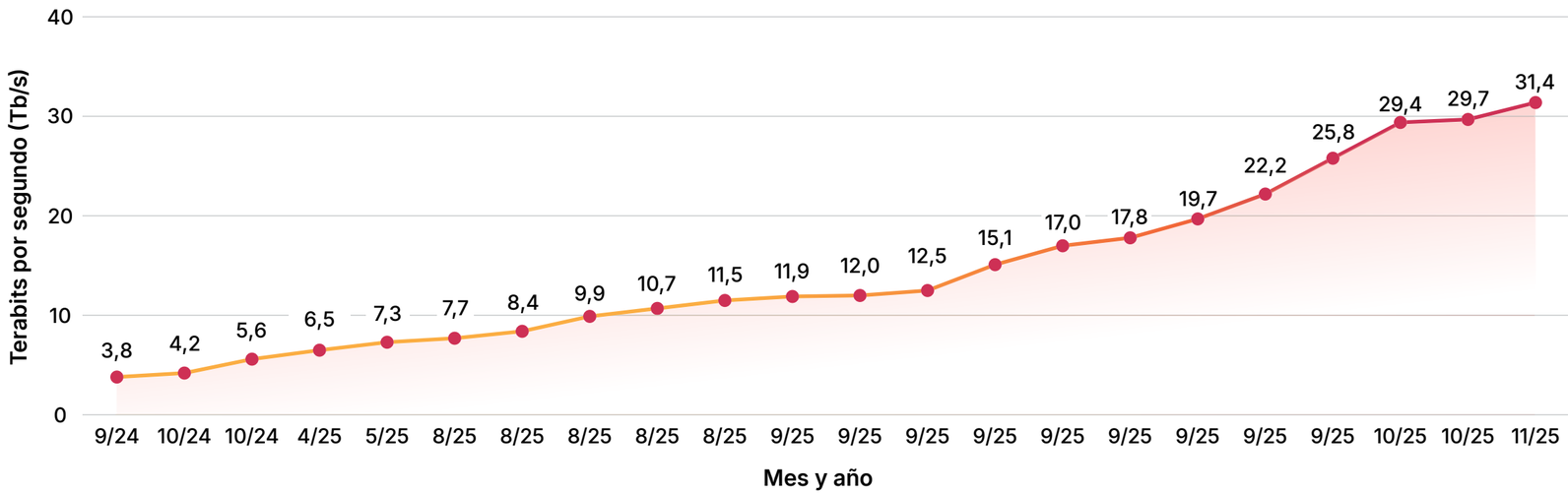
Cuando la velocidad expone las debilidades estructurales

El cambio definitorio de 2026 no es el volumen de vulnerabilidades, sino la velocidad a la que se explotan. Agentic AI ha reducido aún más la ventana entre la divulgación y la explotación, lo que permite a los ciberdelincuentes identificar y poner en práctica las vulnerabilidades en cuestión de días y, cada vez más, en cuestión de horas.

Los datos son claros. En 2025, se observaron 884 vulnerabilidades explotadas activamente, y el 29 % mostró evidencia de explotación el mismo día en que se publicaron.[18] La escala es igualmente sin precedentes. React2Shell, una de las vulnerabilidades más notorias del año, registró más de mil millones de intentos de explotación en solo 11 días.[19]

Escalamiento sin preparación de la arquitectura

Récord mundial de ataques DDoS



Fuente: Cloudflare Radar

En poco más de un año, el mayor ataque DDoS registrado se multiplicó por casi diez. Los sistemas centralizados y estrechamente acoplados nunca se diseñaron para esta escala. La deuda técnica ahora se traduce directamente en fragilidad sistémica bajo la presión de la velocidad de la máquina.

Los entornos heredados están fallando bajo presión. Las fallas importantes a menudo ocurren cuando las dependencias compartidas se rompen al mismo tiempo. Años de soluciones rápidas han creado una deuda oscura: integraciones ocultas, API frágiles y sistemas demasiado riesgosos para parchear. Estos entornos no se crearon para las amenazas a la velocidad de las máquinas ni para la verificación continua.

Esto también expone los límites de los ciclos de revisiones de 30, 60 y 90 días. Las amenazas se explotan en horas, no en trimestres. La protección debe extenderse hacia el perímetro, reduciendo la exposición antes de que los sistemas vulnerables se vean afectados.

> Los atacantes no distinguen entre los sistemas antiguos y los nuevos; **buscan los puntos débiles.** La deuda tecnológica 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 escasez de innovación

Las organizaciones con pilas obsoletas están atrapadas en un ciclo de escasez de innovación. A medida que la infraestructura se vuelve más frágil, aumentan los incidentes de seguridad. A medida que aumentan los incidentes, se desvía más presupuesto y talento al mantenimiento. El resultado es una reserva cada vez más reducida de capacidad de crecimiento.

La empresa global promedio desperdicia más de USD 370 millones por año debido a su incapacidad para modernizar de manera eficiente los sistemas y 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 los líderes utilizan la IA para acelerar la diferenciación, los rezagados pagan una "tasa de interés" cada vez mayor por el código antiguo 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 supone automatización, integración y control en tiempo real. Los sistemas heredados asumen intervención manual, configuraciones estáticas y 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 con la aplicación de parches lenta y con 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 las bases débiles para las operaciones impulsadas por IA. Esto a menudo obliga a un equilibrio entre el riesgo cibernético y el riesgo operativo, una tensión familiar entre los Directores técnicos y los CISO cuando la aplicación de parches podría interrumpir el negocio. El resultado es un retraso, y el retraso es exactamente lo que explotan las amenazas a la velocidad de las máquinas.

Las organizaciones están retrasando la adopción de la IA no porque carezcan de ambición, sino porque su infraestructura no puede admitirla de manera segura. Mientras tanto, los competidores con arquitecturas modernizadas permiten que las iniciativas de IA impulsen la modernización, utilizando 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 normativo de la seguridad, en comparación con el 35 % de las que están atrasadas.[22]

USD 370 millones

desperdiciados por año debido a la incapacidad de modernizar de manera eficiente los sistemas y aplicaciones heredados obsoletos e ineficientes.[23]

La brecha del liderazgo

La diferencia entre los líderes y los rezagados es la disciplina en las decisiones. Las organizaciones que escapan de la trampa de la deuda toman decisiones difíciles al principio. Centralizan la autoridad de modernización, alinean la seguridad con la resiliencia empresarial y tratan la arquitectura como un activo estratégico. El 73 % de los "líderes" de la modernización han centralizado la toma de decisiones con solo unas pocas personas, en comparación con solo el 36 % de los "rezagados".[24] Aquellos que fracasan quedan atrapados en la parálisis impulsada por los comités, donde las vulnerabilidades se mueven más rápido que las decisiones y los riesgos se agravan mientras los planes se debaten sin cesar.

La deuda técnica a menudo refleja la deuda organizacional. La propiedad fragmentada, la responsabilidad poco clara y las decisiones diferidas crean la misma fragilidad en los modelos operativos y de liderazgo que existe en la infraestructura heredada. En 2026, ya no se podrá sobrevivir a esa fragilidad.

La modernización como reducción de riesgos: recuperar el tiempo

Escapar de la trampa de la deuda requiere ver la modernización como un mandato de resiliencia, en lugar de un ciclo de actualización de TI. La modernización reduce el riesgo mediante la reducción de la superficie de ataques por consolidación, lo que permite la aplicación automatizada de parches y respuestas, y hace que la defensa y las operaciones basadas en IA sean viables a gran escala. Y lo que es igualmente importante, reasigna los escasos recursos de ingeniería a trabajos de alto valor, en lugar de 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 establecida, los sistemas se pueden perfeccionar, ampliar y adaptar rápidamente, sin acumular nuevas capas de fragilidad.

El cambio requerido no es gradual. Exige alineación ejecutiva y medidas decisivas. La arquitectura heredada debe tratarse como un riesgo comercial cuantificado, no como un inconveniente técnico. La autoridad de decisión para la modernización debe estar centralizada. Las iniciativas de IA permiten la renovación de la arquitectura en lugar de esperar a que se den las condiciones perfectas. Las plataformas deben consolidarse para reducir la complejidad y restaurar la visibilidad.

En última instancia, la modernización consiste en recuperar tiempo: tiempo para innovar, tiempo para responder y tiempo para competir antes de que la acumulación de riesgos erosione la ventaja.

73 %

de los "líderes" de la modernización han centralizado la toma de decisiones con solo unas pocas personas, en comparación con solo el 36 % de los "rezagados".[25]

PREGUNTAS PARA EL EQUIPO DIRECTIVO

El costo compuesto de la arquitectura heredada

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

P1

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

¿Quién es el responsable de solucionarlos y cuál es el plazo para reducir ese riesgo?

P2

¿Qué porcentaje del gasto en seguridad se destina a mantener sistemas heredados y qué porcentaje a reconstruir la resiliencia?

¿Cuál es nuestra mezcla objetivo en los próximos 12-24 meses?

P3

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

¿Qué ganancias en ingresos, eficiencia o riesgo estamos aplazando como resultado?

P4

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

¿Cómo mediremos el progreso y exigiremos responsabilidades a los líderes?

P5

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

¿Se trata de límites presupuestarios, carencias de talento, prioridades contrapuestas o propiedad poco clara? ¿Cuál eliminaremos primero?

6

Espejismo en la nube: Desacoplamiento del riesgo en cascada

Espejismo en la nube: Desacoplamiento del riesgo en cascada

A medida que las empresas se consolidan en menos plataformas en la nube para avanzar más rápido, muchas aumentan silenciosamente el riesgo sistémico. Las estrategias de nube única simplifican las operaciones, pero concentran los puntos de fallo, mientras que la multinube a menudo se trata como una casilla de verificación en lugar de una estrategia de resiliencia diseñada.

Las recientes interrupciones han hecho que una verdad sea inevitable: la resiliencia no está determinada por la cantidad de nubes que 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 resilientes por diseño, creadas para contener los fallos, limitar el radio de explosión y preservar la confianza bajo presión.

Cuando la velocidad se convierte sutilmente en fragilidad

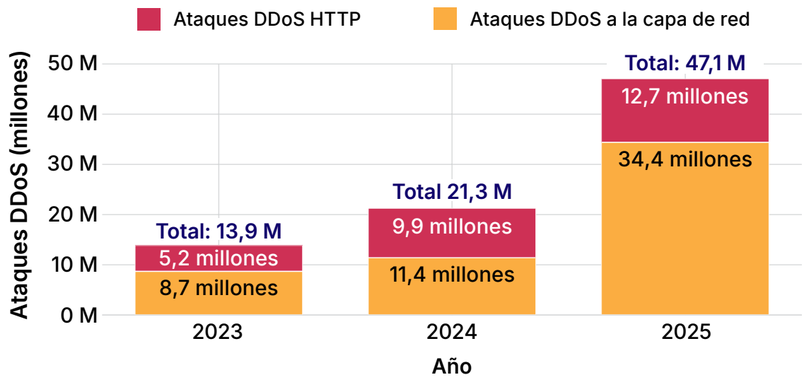
La empresa moderna no tenía la intención de crear sistemas frágiles. La adopción de la nube prometió velocidad, elasticidad y fiabilidad, pero también introdujo un riesgo de concentración más discreto: menos visible, más sistémico y más difícil de resolver en condiciones de estrés.

Las interrupciones actuales no se deben únicamente a fallas de un solo proveedor. Un incidente de un solo proveedor puede seguir siendo el desencadenante, pero los eventos más disruptivos se producen cuando las dependencias compartidas fallan 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 informadas públicamente involucran a proveedores externos de centros de datos o de TI, incluidos gigantes de la nube e Internet, empresas de telecomunicaciones y colocación.[26]

Con demasiada frecuencia, la continuidad del negocio sigue estando centrada en la recuperación, en la restauración del servicio en lugar de en la contención de los fallos. Con el tiempo, las dependencias en capas convierten los entornos en sistemas estrechamente acoplados en los que los pequeños fallos pueden producirse en cascada. Por lo general, esta fragilidad solo se hace visible en una crisis.

Presión permanente

Ataques DDoS por año y tipo



Fuente: Cloudflare Radar

La actividad DDoS se ha más que triplicado en dos años. La interrupción a gran escala ya no es episódica, es continua. En entornos estrechamente acoplados, la presión externa sostenida expone las dependencias ocultas y amplifica los pequeños fallos hasta convertirlos en eventos sistémicos. La resiliencia debe asumir un estrés constante, no una falla rara.

> La nube crea escala, **pero no automáticamente resiliencia**. Si tus sistemas fallan a la vez, no están diseñados para la redundancia. Están diseñados 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 fallas obtienen resultados sustancialmente mejores. Una gran empresa de servicios financieros redujo las interrupciones en un 40 % y redujo los tiempos de resolución en casi un 60 % después de modernizar la arquitectura, mejorar la observabilidad y la ingeniería para la preparación ante fallas.[27]

En la actualidad, las interrupciones no se deben tanto a la ruptura de la nube como a la erosión de la independencia. El riesgo real es el acoplamiento arquitectónico. La resiliencia ahora requiere aislamiento intencional, límites de radio de explosión y tratar la contención de fallas como un principio de diseño central.

La ilusión de la nube única: eficiencia sin contención

Para muchas organizaciones, las estrategias de la nube única se han convertido en la opción predeterminada en la búsqueda de la eficiencia. Las herramientas estandarizadas reducen la complejidad, aceleran la implementación y reducen los costos operativos. La contrapartida es el riesgo de concentración. La misma consolidación que impulsa la eficiencia también puede centralizar los fallos.

Los principales proveedores de servicios en la nube suelen ser muy resilientes, pero el mayor riesgo actual es de tipo arquitectónico y operativo. Cuando la identidad, la aplicación de políticas, la observabilidad y las tuberías de entrega dependen del mismo plano de control o límite de confianza, la resiliencia se convierte en una suposición en lugar de una propiedad inherente. Un solo error, ya sea del lado del proveedor o del lado del cliente, puede propagarse ampliamente si el diseño no lo contiene. Pueden existir planes de recuperación, pero la verdadera contención a menudo no existe. Cuando algo falla, demasiadas cosas fallan a la vez.

Los datos de la industria refuerzan esta realidad. Un estudio de Gartner muestra que la mayoría de los fallos en la nube se deben a errores de configuración y problemas operativos, más que a defectos de la infraestructura central. 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 proyecciones sugirieron que para el año pasado, hasta el 99 % de los fallos en el entorno de 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 es clara. La resiliencia debe ser diseñada, no asumida. Eso significa diseñar tanto para la contención como para la recuperación, separando las dependencias críticas, agregando medidas de seguridad y políticas como código para reducir el impacto de los errores, y probando regularmente los escenarios de falla. El riesgo de concentración no ha desaparecido en la era de la nube. Ha subido en la pila. Las organizaciones que siguen siendo resilientes son aquellas que garantizan que un solo fallo no se convierta 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, solo entre logotipos. La mayoría de los entornos multinube comparten proveedores de identidad, canalizaciones de CI/CD, herramientas del marco de control y dependencias de SaaS. Cuando esas capas compartidas fallan, la promesa de independencia se evapora instantáneamente. 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 se trata de cuántas nubes hay en un diagrama. Se trata de qué capas fallan de forma independiente bajo presión, y cuáles no.

Ingeniería para la contención, no para la perfección

El diseño autónomo comienza con la expectativa de que los sistemas fallarán y se centra en mantener las fallas acotadas y útiles mientras se aprende. El objetivo no es solo resistir los impactos, sino mejorar gracias a ellos.

La contención es lo que lo hace posible. Significa que una falla en un área no se extiende automáticamente a otras. Una falla aislada tiene un alcance limitado, una causa clara y un impacto manejable. No afecta la identidad, la política, los datos y las operaciones de forma conjunta.

Las organizaciones que utilizan la IA y la automatización de forma extensiva acortaron considerablemente los ciclos de vida de las fugas en **80 días** y redujeron los costos promedio de las fugas.

USD 1,9 millones[29]

Esto se refleja en la arquitectura a través de la independencia entre las capas de identidad, políticas y 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 mantenerlos locales, explicables y con capacidad de supervivencia, y utilizarlos para fortalecer el sistema. Las organizaciones líderes no son aquellas con cero incidentes, sino aquellas que limitan con éxito el radio de explosión de cualquier evento concreto.

La contención como ventaja para el crecimiento

Aunque a menudo se considera un seguro, la disociación de capas favorece la velocidad y el crecimiento. El informe de IBM de 2025 sobre el costo de las fugas de datos reveló que las organizaciones que utilizan IA y automatización acortaron considerablemente los ciclos de vida de las fugas de datos en 80 días y redujeron los costos promedio de las fugas de datos en USD 1,9 millones.[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 escalamientos ejecutivos. Cuando se contiene el fracaso, los líderes mantienen la capacidad de decisión.

La contención no es defensiva. Permite actuar con mayor rapidez y asumir riesgos de forma más inteligente en un entorno volátil.

Diseñar pensando en los fallos desde el principio

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

Los ejecutivos deben dejar de preguntarse con qué rapidez podemos recuperarnos, para centrarse en lo que no puede fallar al mismo tiempo. Eso requiere claridad sobre los planos de control compartidos, las dependencias de identidad y las canalizaciones, además de evidencia de pruebas de modo de falla, no solo el tiempo de actividad. La contención pertenece al nivel de la junta directiva porque la falla sistémica es un riesgo comercial; no se puede delegar. Debe diseñarse deliberadamente desde arriba para que ningún fallo único se convierta en un evento de toda la empresa y cada incidente fortalezca el sistema.

> **Los atacantes buscan una debilidad para desencadenar una cascada. Si un único riesgo se convierte en un evento empresarial, no es mala suerte. Eso es diseño arquitectónico".**
>
> **Dave Trader, director de seguridad de la información, HALO Branded Solutions**

PREGUNTAS PARA EL EQUIPO DIRECTIVO

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

Debatidas en conjunto, estas preguntas revelan si la empresa puede contener la interrupción en tiempo real o si la estabilidad aún depende de la esperanza, de esfuerzos extraordinarios y de la recuperación posterior a un incidente.

P1

¿Qué sistemas críticos pueden fallar sin detener el negocio?

¿Hemos demostrado esto mediante pruebas, o es teórico?

→

P2

Si fallara la identidad o una plataforma central, ¿qué ingresos se detendrían?

¿Conocemos el impacto por adelantado o solo después de la interrupción?

→

P3

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

¿En qué aspectos hemos reducido la dependencia y en cuáles sigue existiendo?

→

P4

¿Estamos midiendo la contención o solo el tiempo de recuperación?

¿Nuestros KPI premian la prevención o la limpieza reactiva?

→

P5

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

¿El impacto fue limitado por diseño o por una circunstancia afortunada?

CONCLUSIÓN

Los principios de liderazgo para una ventaja duradera

En un mundo determinado por las decisiones impulsadas por la IA, los sistemas autónomos y los ecosistemas digitales profundamente interdependientes, la resiliencia ya no es suficiente. La ventaja provendrá de la capacidad de los sistemas para detectar el estrés, adaptarse en tiempo real, contener los fallos y seguir funcionando sin esperar la intervención humana. Esto es lo que llamamos resiliencia autónoma.

Este informe no es un inventario de amenazas. Define un mandato de liderazgo: identificar y abordar las fallas integradas en las empresas modernas. Estas debilidades estructurales pueden parecer manejables en condiciones de estado estable, pero seguramente saldrán a la superficie bajo presión sin una acción decisiva. Subyacen a 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.

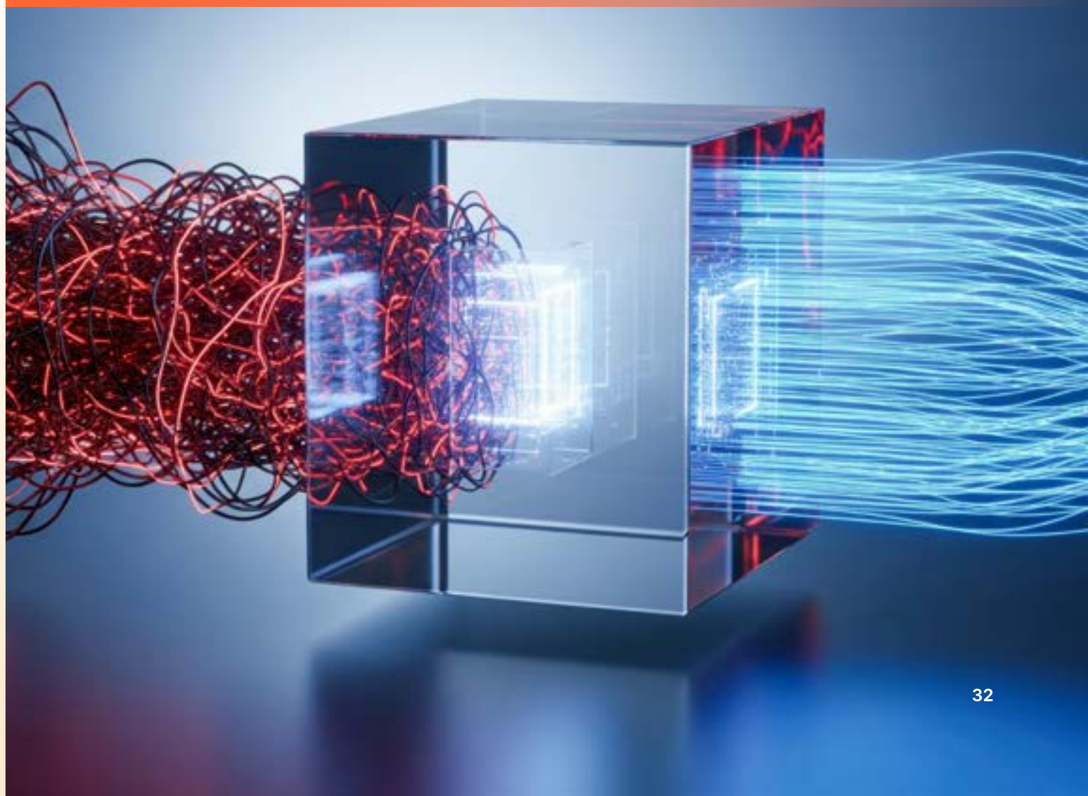
Enfrentar estas fallas no es competencia exclusiva del CISO. La resiliencia autónoma es una responsabilidad de los altos directivos, determinada por la forma en que los equipos ejecutivos establecen prioridades, asignan autoridad y diseñan sistemas que se autorregulan. Las organizaciones autónomas se distinguen por los principios que sus equipos directivos encarnan sistemáticamente:

- **Apropiación compartida del riesgo sistémico en lugar de una responsabilidad delegada.** El riesgo sistémico es propiedad del equipo directivo, no se delega en el organigrama. La responsabilidad es explícita, la propiedad se comparte entre los altos directivos y los consejos se involucran a través de escenarios y compensaciones reales, no de informes estáticos.
- **Ejecución integrada en los sistemas por encima de la intención declarada.** Las decisiones solo importan si se ejecutan a la velocidad de la máquina. El control de los modelos, los datos, los prompts y las acciones autónomas debe residir donde se produce la ejecución. Cualquier cosa que dependa de la documentación, la alineación o el proceso manual no podrá escalar.
- **Independencia estructural por encima de la conveniencia a corto plazo.** Lo que se siente eficiente en condiciones de calma a menudo crea fragilidad bajo estrés. 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 las cascadas se convierte en una ventaja estratégica.
- **Confianza demostrable frente al control asumido.** La confianza debe ser continuamente demostrable, no implícitamente asumida. Los directivos exigen visibilidad del comportamiento del sistema, controles exigibles de las identidades de personas y máquinas, y pruebas de integridad a la velocidad de las máquinas. La supuesta confianza falla bajo la autonomía.
- **Los fracasos como aprendizaje.** El error se espera y se utiliza deliberadamente como entrada. La detección temprana, el radio de explosión limitado, la recuperación rápida y el aprendizaje institucional definen el rendimiento del liderazgo. La métrica que realmente importa no es la prevención, sino la velocidad de recuperación.

En 2026, el liderazgo se define menos por la planificación para la estabilidad y más por el diseño para la disrupción.

Las organizaciones líderes serán aquellas cuyos ejecutivos incorporen estos principios en las decisiones diarias, convirtiendo la volatilidad en aprendizaje, la presión en progreso y la incertidumbre en ventajas.

Las organizaciones que lideren serán aquellas cuyos ejecutivos incorporen estos principios en las decisiones diarias: **convirtiendo la volatilidad en aprendizaje, la presión en progreso y la incertidumbre en ventaja.**



Acerca de Cloudflare

ACERCA DE CLOUDFLARE

Una plataforma. Una red programable.

+330 ciudades
en +125 países, incluida China continental

↳ **con +210 ciudades**
con GPU para inferencia de IA en todo el mundo

~50 m/s
de distancia de ~95 % de la población mundial conectada a Internet

~13 000 redes
se conectan directamente a Cloudflare, lo que incluye ISP, proveedores de servicios en la nube y grandes empresas

477 Tb/s
de la capacidad de la red y sigue creciendo

ACERCA DE CLOUDFLARE

Ecosistema de seguridad de Cloudflare

Resiliencia y protección perimetral

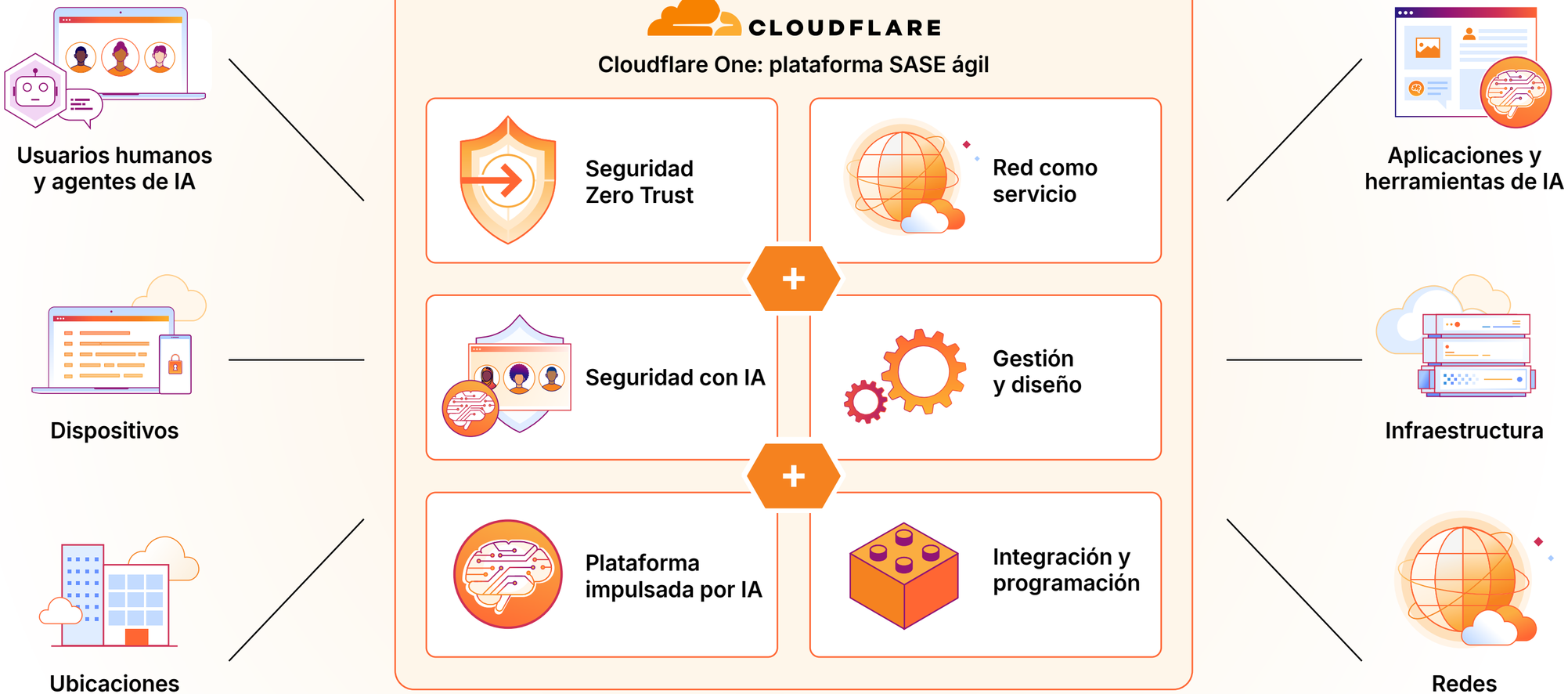
- Protección de aplicaciones web y API: bloquea ataques, detecta vulnerabilidades y mejora la disponibilidad.
- Servicio de seguridad en el perímetro (SSE): aplica la seguridad Zero Trust en todos los equipos híbridos.
- Mitigación de DDoS: resiste los ataques más grandes y avanzados con 477 Tb/s de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

Integración segura de la nube y la red

- Servicio de acceso seguro (SASE): Conecta y protege a tus usuarios, agentes de la e infraestructura.
- Red como servicio y multicloud: Conecta, protege y acelera tus redes corporativas sin el costo y la complejidad del hardware heredado.
- Interconexión de red: conecta directamente tus redes locales y en la nube a la red de Cloudflare.

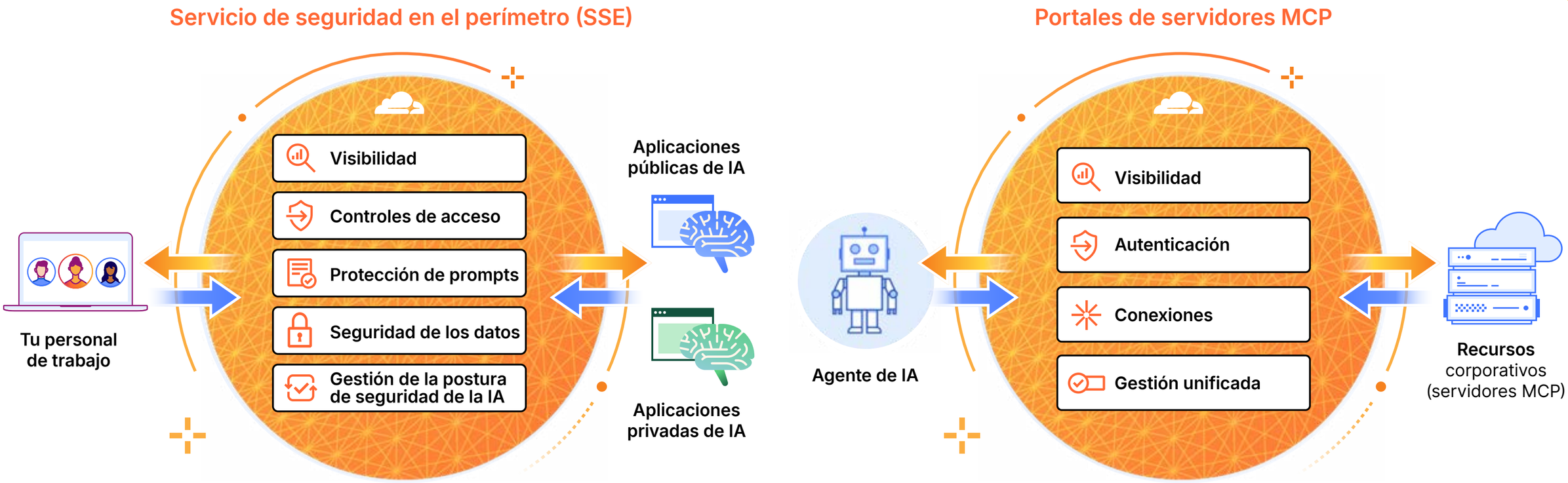
ACERCA DE CLOUDFLARE

Servicios Cloudflare One



ACERCA DE CLOUDFLARE

Proteger el uso de la IA generativa y controlar los agentes de IA



ACERCA DE CLOUDFLARE

Servicios de IA de Cloudflare en todo el ciclo de vida

ACERCA DE CLOUDFLARE

Información para los directivos ejecutivos nivel modernos

Navegar por el panorama de amenazas actual y los rápidos cambios tecnológicos requiere más que conocimiento operativo, exige previsión estratégica. "The Executive Lens" de Cloudflare es un centro de recursos dedicado específicamente para los directivos ejecutivos.

Descubre información de expertos, marcos prácticos e investigaciones exclusivas sobre temas empresariales fundamentales como la ciberresiliencia, la gestión segura de la IA y la transformación digital global.

Leer The Executive Lens hoy.

Más información

Recursos adicionales

Forrester Total Economic Impact

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

Más información

Security Signal

Identifica lo que realmente importa y enfócate en las tendencias clave de ciberseguridad actuales. Cada episodio de Security Signal traduce las complejidades de la ciberseguridad en inteligencia práctica para los ejecutivos a cargo.

Ver ahora

Informe sobre amenazas de Cloudflare 2026

El panorama de amenazas de 2026 se define por una nueva medida de eficacia (MOE, por sus siglas en inglés). Este informe detalla los nuevos riesgos del posicionamiento previo patrocinado por el estado, el robo de tokens, los ataques DDoS hipervolumétricos, etc.

Más información

theNET

Información sobre la innovación en ciberseguridad, el panorama de las amenazas y el futuro de Internet con perspectivas ejecutivas sobre cómo resolver los desafíos organizacionales con la tecnología.

Más información

the NET BY CLOUDFLARE

Referentes

	Global	América	Europa, Oriente Medio y África	Asia Pacífico	Japón
Líderes 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
Directores ejecutivos	 **Ramy Houssaini** Director de soluciones de seguridad ramy@cloudflare.com	 **Khalid Kark** Director de informática, América khalid@cloudflare.com	 **Christian Reilly** Director de informática, EMEA creilly@cloudflare.com	 **Volker Rath** CISO de campo volker@cloudflare.com	 **Koichiro Otobe** Director de tecnología de campo, Japón koichiro@cloudflare.com

CLOUDFLARE

2026

Informe Security Signals de Cloudflare

Resiliencia autónoma

+55 (11) 32304523 | enterprise@cloudflare.com | www.cloudflare.com/es-la/

REV:BDES-8897.19MAR2026

Referencias

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, "tráfico de bots", 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, Informe sobre el costo de una fuga de datos, 2024
8. Lareina Yee, et al., “The AI Reckoning: How Boards Can Evolve”, McKinsey y 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, Informe sobre el costo de una fuga de datos, 2024
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 innovación de aplicaciones de Cloudflare 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. Instituto SANS.
16. Instituto SANS.
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. Red global de Cloudflare: Datos.
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, "Encuesta global de ejecutivos de tecnología: la deuda técnica, una carga importante", www.protiviti.com/us-en/global-technology-executive-survey-tech-debt-major-burden. Consultado el 11 de febrero de 2026.
22. Cloudflare, "Informe de Innovación de Aplicaciones de Cloudflare 2026".
23. Pegasystems, “Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research”.
24. Cloudflare, "Informe de Innovación de Aplicaciones de Cloudflare 2026".
25. Cloudflare, "Informe de Innovación de Aplicaciones de Cloudflare 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”.