CLOUDFLARE

2025

Informe Cloudflare Signals

Resiliencia a gran escala

PRÓLOGO DE MICHELLE ZATLYN

Vivimos tiempos sin precedentes. La tecnología avanza a un ritmo vertiginoso.

Desde el auge explosivo de la IA generativa, llena de promesas y temores, hasta las ciberamenazas cada vez más presentes, y desde la nueva paradoja de un mundo hiperconectado hasta las implicaciones para las sociedades locales y la economía global, la única constante parece ser el cambio. Las reglas del juego están en constante evolución, y si no ajustamos continuamente nuestro manual de estrategias, pronto quedará obsoleto.

Por eso, me complace presentar la primera edición del ***informe Cloudflare Signals***, un informe anual que describe las tendencias de ciberseguridad y las conclusiones fundamentales para crear un plan de acción adecuado para ti.

Cloudflare protege el 20 % de los sitios web del mundo y bloquea una media de más de 227 000 millones de ciberamenazas al día. Eso nos ofrece una perspectiva muy interesante. No vemos solo datos, sino también patrones, comportamientos y puntos de inflexión que nos indican el rumbo global.

Qué sabemos con certeza: las amenazas basadas en la IA requieren una protección basada en la IA. La seguridad Zero Trust debe ser la norma. La preparación poscuántica no es un problema del mañana, se debe lograr ya. Y todo esto requiere la participación y el respaldo del equipo directivo. **La resiliencia no es opcional, es esencial.**

El ***informe Cloudflare Signals*** está diseñado intencionadamente para proporcionar información sobre las fuerzas que configuran el panorama de la seguridad. Nuestro objetivo es que todas las empresas (sea cual sea su tamaño), los gobiernos y los particulares de todo el mundo tengan los conocimientos necesarios para tomar decisiones que les permitan optimizar la resiliencia.

Nuestra misión es ayudar a mejorar Internet, y eso empieza por ayudarte a tener éxito.

Michelle Zatlyn
Cofundadora y presidente,
Cloudflare

RESUMEN EJECUTIVO

En 2025, la resiliencia a gran escala ya no es opcional, es una prueba definitoria de liderazgo.

A medida que aumenta la complejidad de las amenazas digitales y se agrava la volatilidad geopolítica, todas las áreas de la empresa (finanzas, operaciones, conformidad, reputación) afrontan una mayor exposición. Los ataques basados en IA, el cambio de los marcos normativos y la expansión de los ecosistemas digitales exigen una respuesta coordinada del equipo directivo.

El *informe Cloudflare Signals 2025* destaca cinco desafíos que requieren integrar la resiliencia (en lugar de añadirla posteriormente). Juntos, identifican la nueva misión de los equipos ejecutivos: integrar la resiliencia en los pilares de la estrategia operativa, de innovación y de crecimiento de la empresa, a gran escala.

Los líderes empresariales expertos observan un cambio evidente: la resiliencia ya no es responsabilidad de una sola función laboral, sino una prioridad estratégica que comparte todo el equipo directivo. Las empresas líderes están dejando atrás la protección reactiva y adoptan entornos tecnológicos proactivos, basados en la información, escalables e integrados en toda la empresa. Aquellos que aborden la resiliencia como una responsabilidad compartida del equipo directivo y como un motor de crecimiento, y no solo como una protección, estarán mejor posicionados para el liderazgo en un mundo cada vez más volátil.

Este informe destaca el compromiso de Cloudflare de crear un ecosistema digital seguro, eficaz y resiliente a gran escala, que permita a empresas de todos los tamaños hacer frente a las interrupciones y operar con confianza a escala global.

Cinco desafíos críticos

que requieren integrar la ciberresiliencia (en lugar de añadirla posteriormente).

1

Las amenazas y los riesgos internos basados en la IA

requieren una estrecha **colaboración entre los directores técnicos**, ya que los ciberdelincuentes ahora utilizan la IA para automatizar y escalar los ataques más rápido de lo que las soluciones de protección tradicionales pueden responder. Las amenazas basadas en la IA requieren una protección basada en la IA, con capacidad de adaptación en tiempo real. La automatización de estas funciones no solo aumenta la cobertura. También permite a las organizaciones escalar su protección sin ralentizar su actividad empresarial.

2

La seguridad Zero Trust, la protección de la identidad y la complejidad de la nube

requieren **el liderazgo de los directores de informática**, ya que las empresas abandonan los modelos basados en el perímetro y adoptan marcos que priorizan la identidad. La seguridad Zero Trust es el estándar de facto para la gestión de riesgos escalable y nativa de nube. Esto garantiza la facilidad de uso, la visibilidad y el control de todos los sistemas distribuidos.

3

La resiliencia ya no es opcional

para **los directores financieros y los directores de gestión de riesgos**. Ante el aumento del riesgo relacionado con terceros y la ampliación de los marcos normativos, los responsables financieros y de la gestión de riesgos deben garantizar que las inversiones van más allá de la mitigación, mejorando la continuidad operativa, la automatización del cumplimiento y la gobernanza escalable. La resiliencia a este nivel debe ser proactiva, integrada y rentable, no un conjunto heterogéneo de soluciones específicas.

4

La privacidad de datos y la preparación poscuántica

requieren la **participación de los directores de privacidad** desde el principio. Ahora que la informática cuántica está a punto de descifrar la encriptación tradicional, la preparación de los datos para el futuro requiere acciones inmediatas. Los líderes empresariales deben acelerar la adopción de la criptografía poscuántica para proteger los datos de larga duración y cumplir con las expectativas normativas en constante evolución.

5

El riesgo geopolítico y las ciberoperaciones selectivas

exigen la **implicación directa de los directores generales y del consejo de administración**. El número de campañas patrocinadas por los estados contra directivos, cadenas de suministro y operaciones globales sigue en aumento. La resiliencia debe llegar a lo más alto, gracias a la información en tiempo real, la preparación del equipo ejecutivo y la coordinación transfronteriza.

"Los ataques basados en IA, el cambio de los marcos normativos y la expansión de los ecosistemas digitales exigen una **respuesta coordinada del equipo directivo**".

Contenido

1

Estrategia "mirror match": proteger la empresa en la era de la IA antagónica

Estrategia "mirror match": proteger la empresa en la era de la IA antagónica

Las ciberamenazas basadas en la IA están evolucionando a un ritmo sin precedentes, por lo que los enfoques de seguridad tradicionales resultan ineficaces. Los atacantes utilizan ahora la IA para automatizar los ataques, eludir la detección y explotar las vulnerabilidades más rápido de lo que las organizaciones pueden responder. El cambio de la protección pasiva a la seguridad proactiva basada en la IA ya no es opcional, es esencial.

Los ataques basados en IA ya están causando un impacto real en las empresas. El 74 % de los profesionales de la seguridad informática afirman que las amenazas basadas en la IA están afectando significativamente a sus organizaciones.[1] Las estafas deepfake, como las videollamadas fraudulentas, han causado pérdidas millonarias, como un caso en Australia de robo de 25 millones de dólares.[2] Los ataques de phishing generados por IA son cada vez más convincentes, mientras que el malware mejorado con IA se adapta para evadir las soluciones de seguridad tradicionales.

Más allá de los ataques directos, la IA está fomentando campañas de desinformación, el envenenamiento de datos y la manipulación de modelos, lo que puede poner en riesgo los sistemas basados en IA.

La mejora de la productividad de los atacantes sobrecarga a los equipos de seguridad

Es posible que muchas herramientas de AI no ofrezcan técnicas de ataque innovadoras, pero pueden ayudar a los ciberdelincuentes a mejorar la productividad, la eficiencia y el volumen de los ataques. Estas herramientas aceleran tareas como la elaboración de correos electrónicos de phishing y el uso de "bots de chat oscuros" para ayudar a codificar el malware.

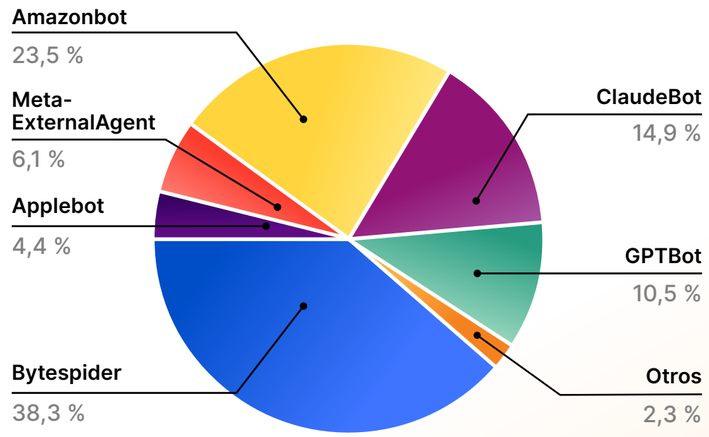
Esto significa que las organizaciones empezarán a afrontar un mayor volumen de ataques, cada vez más sofisticados, que suelen utilizar modernos métodos de ataque. Los procesos de seguridad manuales, como la clasificación de los correos electrónicos de phishing y el ajuste manual de las detecciones para detener las últimas amenazas, se verán saturados a medida que aumente el volumen de los ataques.

La apropiación de contenido de la IA amenaza a los creadores de contenido digital

Los modelos de IA necesitan datos con los que entrenarse, y muchas empresas de IA recopilan esta información mediante la extracción web automatizada. De hecho, los rastreadores de IA ya representan el 2 % de todo el tráfico de bots que Cloudflare procesa en nuestra red.[3]

El contenido derivado de la IA puede desviar el tráfico y las interacciones de los sitios web. Esto puede perjudicar gravemente a las organizaciones que dependen del contenido y la publicidad en línea para sus ingresos. El rechazo a estas prácticas es cada vez mayor. En febrero de 2025, la empresa educativa Chegg demandó a Google por perjudicar su tráfico con IA, y la industria creativa del Reino Unido lanzó la campaña "Make It Fair" contra el uso no autorizado de contenido.[4]

Principales rastreadores de IA según el porcentaje de tráfico de la capa de aplicación



Casi todo el tráfico de rastreadores de IA **(98 %)** observado por Cloudflare en 2024 **procedía de solo seis empresas.**[5]

Para las organizaciones que dependen en gran medida de la publicación de contenido o publicidad digital, **los bots de apropiación de contenido de IA son una amenaza existencial.**

El fraude de identidad sintética afecta a sectores críticos

La IA está impulsando el auge del fraude de identidad sintética (SIF), en el que los ciberdelincuentes crean identidades hiperrealistas combinando datos reales y falsos para eludir los sistemas tradicionales de verificación. Los datos personales generados por IA, los deepfakes y el relleno automatizado de credenciales dificultan la detección de estas identidades. Esto plantea graves riesgos a sectores muy afectados por estos ataques, como los servicios financieros, la sanidad y los organismos gubernamentales.

A diferencia del fraude tradicional, el fraude de identidad sintética suele pasar desapercibido, ya que no hay víctimas inmediatas, y esto permite a los estafadores crear historiales crediticios y ejecutar estafas a gran escala.

La IA aumenta las amenazas internas

El teletrabajo y la adopción de la nube han ampliado la superficie de ataque de las amenazas internas, lo que dificulta su detección. Más de la mitad de las organizaciones declaran haber sufrido una amenaza interna en el último año, y el 8 % ha afrontado más de 20 incidentes.[6]

Ahora la IA agrava este desafío, ya que proporciona a los usuarios internos herramientas eficaces para eludir la detección. El phishing basado en IA, las estafas deepfake y los ataques automatizados de ingeniería social pueden generar mensajes convincentes y contextualizados en apenas segundos, lo que facilita el engaño y aumenta la frecuencia de los ataques.[7]

No todas las amenazas internas son ataques intencionados. El DBIR de Verizon de 2024 reveló que el 68 % de las fugas de datos se debieron a factores humanos, como engaños sufridos mediante estafas de ingeniería social o errores de las personas.[8] El phishing de objetivo definido asistido por IA aprovecha estos errores, imitando a colegas o ejecutivos reales con una precisión casi perfecta para intentar engañar a los empleados con el objetivo de que compartan sus credenciales, aprueben transacciones o expongan datos confidenciales.

Para identificar estos riesgos antes de que el impacto sea mayor, las organizaciones deben implementar funciones de análisis del comportamiento, supervisión en tiempo real y detección de anomalías. La automatización de la seguridad basada en la IA es ahora imprescindible para igualar la velocidad y la escala de las amenazas basadas en la IA.

Los bots de IA redefinen el panorama de la ciberseguridad

Los bots de IA están aumentando tanto la sofisticación de los ataques como la exposición al riesgo. En 2024, el 28 % de todo el tráfico de aplicaciones observado por Cloudflare procedía de bots, una cifra que se ha mantenido estable en torno al 30 % durante los últimos cuatro años. Aunque los bots pueden servir para fines legítimos, como la automatización de los servicios al cliente y la indexación de los motores de búsqueda, la gran mayoría (93 %) no están verificados y son potencialmente maliciosos.[9]

Lo que supone un cambio muy importante son los bots de IA que permiten ataques automatizados a gran escala con una eficiencia sin precedentes. Los atacantes utilizan ahora bots para llevar a cabo el relleno de credenciales, lanzar ataques de denegación de servicio distribuido (DDoS), extraer datos confidenciales y ejecutar fraudes a velocidad de máquina. Los modelos de IA potencian estas capacidades, ya que pueden generar intentos de phishing realistas, eludir los desafíos CAPTCHA tradicionales y evitar la detección con un comportamiento adaptable.

La automatización de la seguridad basada en la IA es ahora **imprescindible** para igualar la velocidad y la escala de las amenazas basadas en la IA.

28 %

de todo el tráfico de aplicaciones observado por Cloudflare **procedía de bots**

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Desarrollar una capacidad defensiva basada en la IA

Para anticiparse a las amenazas basadas en la IA, las organizaciones deben adoptar un enfoque proactivo que prevenga y mitigue estas amenazas en tiempo real. **Estas son algunas preguntas que puede plantear el equipo directivo para evaluar la preparación de la organización.**

P1

¿Utilizamos la IA para mejorar la observabilidad integral de la seguridad?

¿Unificamos los registros, los análisis, las alertas y los análisis forenses en una única interfaz para identificar los riesgos y su causa principal?

P2

¿Aprovechamos la seguridad basada en la IA para detectar y neutralizar las amenazas en tiempo real?

¿Disponemos de detección basada en IA para analizar grandes conjuntos de datos, identificar las anomalías y automatizar la respuesta a las nuevas amenazas?

P3

¿Hasta qué punto estamos protegidos contra el phishing basado en IA, los deepfakes y el malware?

¿Implementamos la detección basada en IA, la autenticación resistente al phishing y controles de seguridad adaptables para combatir los ataques en constante cambio?

P4

¿Protegemos nuestros datos privados contra los bots de apropiación de contenido de IA y las amenazas automatizadas?

¿Disponemos de soluciones de gestión de bots, autenticación de API y marca de agua digital para evitar el robo y la explotación de datos?

P5

¿Aprovechamos el análisis del comportamiento basado en IA para detectar las amenazas internas en tiempo real?

¿Analizamos sistemáticamente el comportamiento de los usuarios, como los patrones de acceso, la escalada de privilegios y los intentos de exfiltración de datos?

PERSPECTIVAS DE LOS DIRECTIVOS

Las nuevas medidas de protección de la seguridad de datos de la IA

Dane Knecht
Director técnico, Cloudflare

Protección de los datos en la era de la IA: confianza, acceso y visibilidad

Hoy en día, el desafío más urgente para las organizaciones es el acceso a los datos, en concreto, cómo gestionarlo y protegerlo en una empresa con cada vez más herramientas de IA. La IA generativa está cada vez más integrada en los flujos de trabajo. Por lo tanto, el desafío ya no es solo reaccionar a las amenazas, sino evitar el acceso que implique un riesgo o el acceso no autorizado a los datos confidenciales.

Esto plantea preguntas urgentes al consejo de administración y al equipo directivo. ¿Cómo concedemos a las herramientas un acceso seguro a los datos empresariales? ¿Cómo garantizamos que un complemento de IA aparentemente inofensivo no sea una puerta de entrada para la exfiltración de datos? Las consecuencias empresariales y para la reputación son reales, y cada vez mayores.

Lo que no vemos: la Shadow AI y las vulnerabilidades de una gobernanza a ciegas

Un importante punto ciego es la proliferación descontrolada de herramientas de IA en toda la empresa. Los empleados adoptan la IA mucho antes de que se aplique una política formal, y no suelen ser conscientes de los riesgos. Estas implementaciones de Shadow AI eluden las revisiones tradicionales, creando superficies de ataque invisibles y nuevos riesgos relacionados con la conformidad.

Son pocas las organizaciones que han identificado dónde se utiliza la IA. Sin esa visibilidad, es casi imposible gestionar la exposición de los datos o responder eficazmente a los incidentes.

Qué es lo siguiente: el control proactivo y un mayor escrutinio normativo

Entre los próximos 12 a 18 meses, la seguridad empresarial pasará de la detección reactiva de las amenazas a la gobernanza proactiva del acceso y del uso de la IA. El escrutinio normativo aumentará, exigiendo transparencia, supervisión operativa y prácticas eficaces de protección de datos.

Las organizaciones que actúen con rapidez (formando equipos de gobernanza interdisciplinarios, definiendo políticas de uso de la IA e implementando controles de acceso para las herramientas y para los usuarios) reducirán el riesgo y se posicionarán como líderes.

El futuro de la resiliencia no consiste solo en detectar las amenazas, sino en controlar cómo y dónde la IA accede a tus datos.

"Los empleados **adoptan la IA mucho antes de que se aplique una política formal**, y no suelen ser conscientes de los riesgos".

2

Más allá del perímetro: la seguridad Zero Trust, la identidad y la nueva frontera de la seguridad

Más allá del perímetro: la seguridad Zero Trust, la identidad y la nueva frontera de la seguridad

La adopción de los entornos multinube, las plataformas SaaS y las arquitecturas basadas en API ha creado un panorama de seguridad fragmentado, donde los errores de configuración, los riesgos relacionados con la identidad y la Shadow IT exponen a las empresas a cada vez mayores ciberamenazas. En este entorno, la seguridad Zero Trust ha sustituido a los modelos obsoletos basados en el perímetro, y se ha convertido en la base para la protección de las aplicaciones, las cargas de trabajo y los datos en la nube con estrategias de verificación continua centrada en la identidad.

Para adaptarse a los cambios, las organizaciones deben aplicar los principios Zero Trust en todas las plataformas en la nube y SaaS.

La seguridad Zero Trust reemplaza las VPN tradicionales

Con el objetivo de acceder a la red, ahora los ciberdelincuentes lanzan activamente ataques de día cero y por fuerza bruta contra los proveedores de VPN.[10] Ante la desaparición del perímetro de red, las organizaciones adoptan la seguridad centrada en la identidad, y aplican la verificación continua, el acceso de privilegio mínimo y la autenticación contextual en las cargas de trabajo en la nube y las aplicaciones SaaS.

El acceso a la red Zero Trust (ZTNA) es ahora esencial, en sustitución de las VPN heredadas que exponen las empresas a los ataques basados en credenciales, el movimiento lateral y las amenazas internas. Sin la seguridad Zero Trust, las empresas corren el de quedar expuestas a accesos no autorizados, credenciales en riesgo y vulnerabilidades de la cadena de suministro.

Las API: el nuevo vector de ataque

Ahora que el 60 % del tráfico de Internet se basa en las API, las API no seguras son uno de los principales objetivos de los atacantes.[11] Muchas organizaciones no las controlan ni protegen, por lo que quedan expuestas a la exfiltración de datos, el abuso de credenciales y los ataques de inyección. El análisis basado en el aprendizaje automático de Cloudflare reveló que las organizaciones subestiman en una cuarta parte los puntos finales de API, lo que crea un importante punto ciego de seguridad.[12]

Para mitigar los riesgos, las empresas deben adoptar la identificación automatizada de las API, la aplicación de la autenticación y la detección de anomalías basada en la IA para evitar las fugas y las filtraciones de datos.

El análisis basado en el aprendizaje automático de Cloudflare reveló que **las organizaciones subestiman en una cuarta parte los puntos finales de API**

La Shadow IT y los servicios en la nube no gestionados agravan el riesgo

La rápida adopción de servicios en la nube no autorizados dificulta cada vez más a los equipos informáticos la supervisión y la protección eficaces de los entornos en la nube. Los empleados utilizan con frecuencia herramientas de colaboración no autorizadas, exponiendo datos confidenciales y eludiendo las políticas de seguridad corporativas.

Los agentes de seguridad de acceso a la nube (CASB), las herramientas de descubrimiento basadas en IA y la aplicación automatizada de políticas son ahora fundamentales para obtener visibilidad en tiempo real, garantizar el cumplimiento normativo y evitar la exposición no autorizada de los datos.

Seguridad centrada en la identidad: el fin de las contraseñas

Las ciberamenazas son cada vez más sofisticadas, y la identidad sigue siendo uno de los principales vectores de ataque. El 25 % de las intervenciones de respuesta a incidentes de Cisco estuvieron relacionadas con usuarios que aceptaron notificaciones push fraudulentas de autenticación multifactor en el primer trimestre de 2024.[13] Las credenciales en riesgo también han dado lugar a importantes fugas, como el ataque a al menos 160 clientes de Snowflake, entre ellos, Grupo Santander, Ticketmaster y Advance Auto Parts.[14]

Los ciberdelincuentes eluden cada vez más la autenticación multifactor, secuestran sesiones activas y roban credenciales, exponiendo a las empresas a fugas generalizadas y apropiaciones de cuentas.

Desafíos:

- **La reutilización de credenciales pone en riesgo a las empresas:** el 46 % de todos los intentos de inicio de sesión humanos implican credenciales en riesgo, una cifra que se eleva al 60 % en el caso de las organizaciones empresariales.[15] Los atacantes automatizan el relleno de credenciales y acceden fácilmente a los sistemas empresariales.
- **Los ataques automatizados de credenciales aumentan rápidamente:** el 94 % de los intentos de inicio de sesión con credenciales filtradas provienen de bots, que prueban miles de contraseñas robadas por segundo.[16] Sin la mitigación de bots en tiempo real y la autenticación adaptable, las organizaciones siguen siendo muy vulnerables a las fugas a gran escala.
- **Las contraseñas son insuficientes**: las contraseñas estáticas e incluso los métodos básicos de autenticación multifactor son cada vez más ineficaces contra las amenazas modernas, que incluyen la omisión de la autenticación multifactor, el secuestro de sesiones y el robo de credenciales resistentes al phishing. Para combatir estos riesgos, las organizaciones deben adoptar la autenticación sin contraseña, aplicar controles de acceso Zero Trust e implementar claves de seguridad compatibles con FIDO2 para eliminar la dependencia de las credenciales estáticas.

46 %
de todos los intentos de inicio de sesión humanos implican **credenciales en riesgo**

94 %
de los intentos de inicio de sesión con credenciales filtradas proceden de bots, que prueban **miles de contraseñas robadas por segundo**

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Proteger la nube y replantear la autenticación

Ante la aceleración de la adopción de la nube, las organizaciones deben replantearse la seguridad y la autenticación para protegerse contra las amenazas en evolución. Un enfoque Zero Trust, la visibilidad basada en la IA y una protección eficaz de la identidad son esenciales para proteger los servicios en la nube, las aplicaciones SaaS y las API. **Determina el grado de proactividad de tu organización a la hora de abordar estos desafíos con preguntas como:**

P1

¿Aplicamos la seguridad Zero Trust en las nubes, las aplicaciones SaaS y las API?

¿Aplicamos la verificación continua, el acceso con privilegio mínimo y la autenticación basada en riesgos en todos los entornos?

P2

¿Tenemos visibilidad integral de la Shadow IT y de los servicios en la nube no gestionados?

¿Utilizamos herramientas de descubrimiento basadas en IA para detectar aplicaciones no autorizadas y aplicar políticas de seguridad?

P3

¿Nuestras API están protegidas contra el acceso no autorizado y las fugas de datos?

¿Implementamos la detección automatizada de API, los controles de autenticación y la detección de anomalías basada en la IA?

P4

¿Hemos eliminado las vulnerabilidades relacionadas con contraseñas en nuestra estrategia de

¿Estamos adoptando la autenticación sin contraseña, la autenticación multifactor resistente al phishing y la protección de identidad adaptable?

P5

¿Estamos preparados para detectar y responder a los ataques automatizados con credenciales?

¿Podemos implementar las funciones basadas en IA de mitigación de bots, análisis del comportamiento y revocación automatizada de credenciales para evitar el acceso no autorizado?

PERSPECTIVAS DE LOS DIRECTIVOS

Zero Trust para un futuro resiliente

Corey Mahan
Vicepresidente de gestión de productos, Cloudflare

En este momento, el mayor desafío que afrontan las organizaciones es equilibrar la seguridad con la facilidad de uso. El trabajo híbrido ha llegado para quedarse, la adopción de la nube se está acelerando y los usuarios esperan un acceso fácil, independientemente de dónde se encuentren o del dispositivo que utilicen. Pero las arquitecturas tradicionales no pueden adaptarse a los cambios. Vemos como demasiadas empresas dependen de un conjunto heterogéneo de soluciones específicas con escalabilidad insuficiente, lo que causa interrupciones, latencia y la frustración de los usuarios.

Los ejecutivos se plantean una pregunta crítica: ¿Cómo podemos ofrecer un acceso seguro sin ralentizar la actividad empresarial? Esa presión es lo que pone a Zero Trust en primer plano, no solo como un modelo de seguridad, sino como facilitador empresarial.

Errores comunes

Muchas organizaciones empiezan con la intención correcta, pero luego se estancan. Un error común es pensar que comprar una "solución Zero Trust" equivale a implementar una estrategia. No es así. La seguridad Zero Trust implica un cambio de mentalidad y de arquitectura.

Otro problema es asumir que "unificado" es lo mismo que "integrado". Muchas plataformas "integradas" simplemente son productos que se han unido y que no comparten datos, políticas o ni siquiera backends. Esto crea puntos ciegos, especialmente en entornos modernos como las API en la nube, los procesos de DevOps y las aplicaciones de IA.

A esto hemos de añadir la Shadow IT y la Shadow AI, es decir, las herramientas que utilizan los empleados sin que los equipos informáticos lo sepan, lo que crea graves vulnerabilidades relacionadas con la gobernanza.

Qué es lo siguiente (12-18 meses)

En el próximo año, veremos cómo Zero Trust evoluciona de los controles aislados a una capa fundamental que abarcará toda la empresa. El enfoque pasará de la gestión segura del acceso remoto exclusivamente a la unificación de las políticas de identidad, datos y tráfico en todos los entornos. Los responsables ya están optando por plataformas resilientes por diseño, globales por defecto, que automatizan las respuestas y que ofrecen visibilidad en tiempo real. Ahí está el verdadero valor: no solo reducir el riesgo, sino también mejorar la agilidad.

Las organizaciones que tomarán la delantera serán las que integren la seguridad Zero Trust en su base digital, como parte integral de su estrategia segura de desarrollo, escala e innovación.

"Un **error habitual** es pensar que comprar una 'solución Zero Trust' equivale a implementar una estrategia".

3

Más eficacia, no solo mayor seguridad: ampliar la protección a toda la infraestructura, los ecosistemas y la supervisión

Más eficacia, no solo mayor seguridad: ampliar la protección a toda la infraestructura, los ecosistemas y la supervisión

Para garantizar la integridad operativa y la ventaja competitiva, es fundamental mejorar la resiliencia en las redes, las cadenas de suministro y los marcos de cumplimiento normativo.

Sin embargo, hoy en día las ciberamenazas, como los ataques DDoS, son más rápidas, más grandes y más complejas, y van más allá del alcance de las soluciones de protección tradicionales. Al mismo tiempo, las cadenas de suministro digitales exponen vulnerabilidades ocultas, mientras que el entorno normativo es cada vez más exigente y fragmentado.

Para seguir siendo competitivas, las organizaciones deben replantear la ciberseguridad. Deben dejar de considerarla un problema informático, y plantearla como una estrategia de resiliencia empresarial (que abarca toda la infraestructura, los ecosistemas y la supervisión).

Los ataques DDoS aumentan en escala y sofisticación

Los ataques DDoS se han convertido en herramientas de precisión utilizadas por ciberdelincuentes, hacktivistas y estados-nación para interrumpir las operaciones y causar daños a nivel de cumplimiento normativo y para la reputación. Los ataques DDoS paralizan empresas de todos los sectores. En 2024, Cloudflare bloqueó 20,9 millones de ataques DDoS, un 50 % más que en 2023.[17]

La escala y la sofisticación de los ataques DDoS van al alza, y los atacantes aprovechan las botnets, los dispositivos IoT y la automatización basada en la IA para lanzar ataques persistentes y de gran impacto contra servicios digitales críticos.

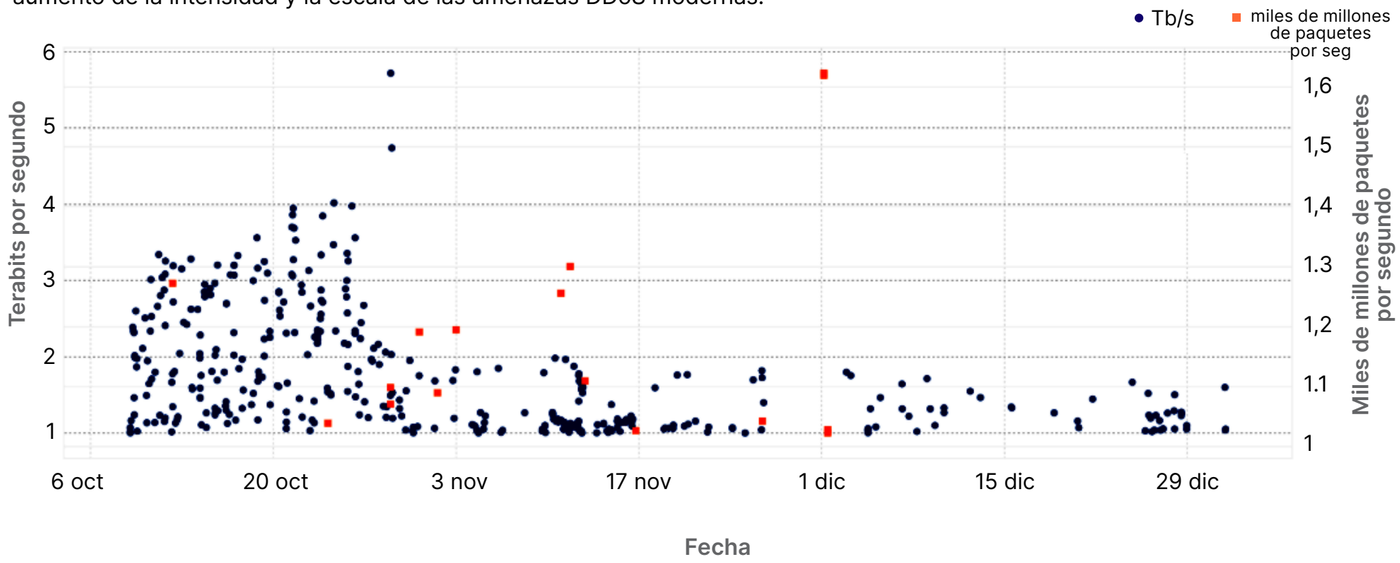
En 2024, Cloudflare bloqueó **20,9 millones** de ataques DDoS, un **50 % más que en 2023.**

Ataques DDoS en 2024

El auge de los ataques DDoS hipervolumétricos

4º trimestre de 2024

En el cuarto trimestre de 2024, los ataques hipervolumétricos a la capa de red alcanzaron niveles sin precedentes. El número de ataques de más de 1 Tb/s se disparó un 1885 % en términos intertrimestrales, mientras que los ataques que superaron los 100 millones de paquetes por segundo (pps) aumentaron un 175 % respecto al trimestre anterior. En concreto, el 16 % de los ataques que superaron los 100 millones de pps también superaron los 1000 millones de pps, lo que pone de manifiesto el aumento de la intensidad y la escala de las amenazas DDoS modernas.[18]



Los datos de Cloudflare muestran que una organización empresarial promedio utiliza **al menos 20 scripts de terceros**

Aumento de los ataques a la cadena de suministro

Según el Foro Económico Mundial, el 54 % de las grandes empresas identifican la gestión de riesgos de terceros como su principal desafío en materia de ciberresiliencia.[19] Los ataques a las cadenas de suministro de software, las plataformas en la nube y las integraciones de terceros están aumentando considerablemente; en 2024, el 15 % de las fugas involucró a un tercero.[20]

La creciente concentración del riesgo en unos pocos proveedores de nube dominantes agrava el problema. Una sola vulnerabilidad o interrupción en uno de estos proveedores puede repercutir en todos los sectores, como lo demuestran las principales interrupciones informáticas de 2024, que causaron pérdidas millonarias y pusieron de manifiesto la fragilidad de los ecosistemas digitales hiperconectados. Estos incidentes fueron un claro recordatorio de que, en el entorno interdependiente actual, un único punto de fallo puede paralizar operaciones enteras.

Un área especialmente vulnerable son los ataques del lado del cliente, en los que las empresas suelen confiar en scripts de terceros para acelerar el desarrollo de aplicaciones web. Estos scripts son código incrustado, a menudo JavaScript, que se origina en un servidor externo.

Si bien estos scripts mejoran la eficiencia, también crean importantes vulnerabilidades de seguridad: cada conexión a funciones externas aumenta el riesgo de ataques a la cadena de suministro basados en el navegador.

Los datos de Cloudflare muestran que una organización empresarial promedio utiliza al menos 20 scripts de terceros, mientras que algunas, sin saberlo, tienen cientos de miles, cada uno de los cuales representa un posible punto de entrada para los atacantes.

Una importante organización de comercio electrónico tenía más de 340 000 scripts de terceros adjuntos a su sitio.[21]

Normativas como la Ley de Resiliencia Cibernética de la UE y la Norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS 4.0) ayudan a abordar la seguridad de la cadena de suministro, pero su aplicación sigue siendo un desafío.

Proliferación de normativas de ciberseguridad

Las normativas en materia de ciberseguridad se están ampliando rápidamente, y esto exige a las empresas una mejora de la seguridad, la transparencia y la notificación de incidentes. La Comisión de Bolsa y Valores de EE. UU. (SEC) exige ahora a las empresas públicas que revelen los incidentes importantes de ciberseguridad y que detallen sus estrategias de gestión de riesgos. El Reglamento General de Protección de Datos (RGPD) de la UE sigue siendo una de las leyes más estrictas en materia de privacidad de datos, e impone sanciones por incumplimiento de hasta el 4 % de los ingresos globales. La CPS 234 de la Autoridad Australiana de Regulación Prudencial (APRA) exige que las instituciones financieras garanticen medidas eficaces de seguridad de la información, mientras que la Ley de Resiliencia Operativa Digital (DORA) de la UE establece normas unificadas de ciberseguridad para el sector financiero.

En otras palabras, la conformidad ya no es un aspecto secundario. Para adaptarse con éxito a este panorama, las organizaciones incorporarán la conformidad en sus operaciones, aprovechando la automatización para agilizar los informes y garantizar siempre su alineación con los cambios de las normativas.

Mayor automatización de la conformidad

Las organizaciones afrontan una complejidad normativa creciente y mayores riesgos operativos, y la automatización de la conformidad se está convirtiendo en una tendencia fundamental. Con más de 52 requisitos en materia de notificación de incidentes de ciberseguridad actualmente activos o propuestos solo en EE. UU., así como marcos globales como el RGPD, DORA y PCI DSS 4.0 que amplían su alcance, los procesos manuales para el cumplimiento normativo han dejado de ser sostenibles.[22] Una encuesta de Deloitte reveló que el 62 % de las organizaciones globales tienen previsto aumentar su inversión en la automatización de la conformidad, aludiendo a la fragmentación normativa y a la necesidad de una respuesta en tiempo real.[23]

Para cumplir con los requisitos de los datos en cada jurisdicción sin sacrificar el rendimiento, las empresas están adoptando la localización estratégica de datos, enrutando el tráfico a través de nodos regionales e implementando herramientas automatizadas de auditoría para verificar la conformidad. Al mismo tiempo, la línea entre la conformidad y la seguridad se está difuminando. Las empresas están implementando marcos integrados que alinean la detección de amenazas, la aplicación de políticas y la preparación para las auditorías.

Esta convergencia permite a las empresas reducir el riesgo, responder más rápido a los cambios normativos y escalar la gobernanza a otros países. Las organizaciones que automaticen y operacionalicen la conformidad se beneficiarán de una ventaja estratégica, ya que acelerarán su entrada en los mercados regulados, mejorarán la confianza de los clientes y minimizarán el riesgo financiero y para la reputación.

El creciente panorama normativo

El marco normativo global para la ciberseguridad y la protección de datos sigue evolucionando rápidamente, y las organizaciones afrontan ahora un complejo entramado de requisitos de conformidad en todas las jurisdicciones.

Por ejemplo:

Reglas de ciberseguridad de la SEC

La Comisión de Bolsa y Valores (SEC) de EE. UU. ha implementado requisitos integrales de divulgación de información sobre ciberseguridad para las empresas públicas. Estas normas exigen la notificación oportuna de los incidentes de seguridad importantes y la divulgación detallada de sus estrategias de gestión de riesgos, gobernanza y experiencia.

NIS2

La directiva NIS2 de la UE establece requisitos de seguridad más estrictos en 18 sectores críticos. Exige medidas en materia de resiliencia, gestión de riesgos, respuesta a incidentes y notificación, con una mayor supervisión y sanciones por incumplimiento.

APRA CPS 234

La norma de seguridad de la información CPS 234 de la Autoridad Australiana de Regulación Prudencial (APRA) exige a las instituciones financieras que garanticen funciones eficaces de seguridad de la información acordes con la dimensión y el alcance de las amenazas a sus activos de información.

DORA

DORA representa el enfoque integral de Europa para la resiliencia operativa digital en el sector financiero. Establece requisitos uniformes para la seguridad de la red y los sistemas de información que respaldan las operaciones de las entidades financieras.

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Replanteamiento de la continuidad y de la conformidad

En un panorama de amenazas determinado por los ataques DDoS a gran escala, la opacidad de las cadenas de suministro y la complejidad de normativas globales, la verdadera resiliencia va más allá de la defensa. Implica diseñar sistemas que sigan funcionando bajo presión, y considerar la conformidad no solo como medida de protección, sino también como un motor estratégico. **Estas cinco preguntas pueden ayudar al equipo directivo a evaluar la preparación de su organización para hacer frente a las interrupciones y adaptarse a ellas.**

P1

¿Nuestra infraestructura puede absorber ataques DDoS a gran escala y garantizar el tiempo de funcionamiento bajo presión?

La capacidad de mitigación debe superar el volumen tanto de los picos de tráfico legítimo como de los mayores ataques registrados. Las organizaciones resilientes implementan una infraestructura con redundancia geográfica y planes de conmutación por error que tienen en cuenta la conformidad, y prueban periódicamente los procedimientos de recuperación para garantizar el tiempo de funcionamiento y la conformidad normativa.

P2

¿Tenemos visibilidad en tiempo real de nuestras dependencias de terceros más críticas?

Las vulnerabilidades de la cadena de suministro son una de las principales causas de los incidentes de seguridad. Las organizaciones con visión de futuro supervisan continuamente a los proveedores y servicios externos, aplican los requisitos de seguridad contractuales e integran la información sobre riesgos de terceros en procesos de gobernanza más generales.

P3

¿Hemos automatizado los flujos de trabajo de conformidad para adaptarnos a los cambios de las normativas globales?

Con tantos marcos normativos en rápida evolución, un enfoque manual de la conformidad no es escalable. Las empresas con un rendimiento óptimo utilizan la auditoría automatizada, la supervisión en tiempo real y el enrutamiento de datos con identificación de jurisdicción para garantizar la alineación continua y reducir los costes.

P4

¿Nuestras funciones de seguridad y conformidad están plenamente integradas?

Los equipos aislados crean ineficiencias y vulnerabilidades. Las plataformas unificadas que alinean la detección de amenazas con los informes normativos agilizan los procesos de auditoría, mejoran la visibilidad y reducen el riesgo en todas las áreas.

P5

¿Hemos probado nuestra postura de resiliencia en su totalidad, desde la detección de incidentes hasta la recuperación y la notificación?

Las organizaciones proactivas desarrollan guías que vinculan los controles técnicos con los requisitos normativos, simulan periódicamente interrupciones y adaptan arquitecturas de conformidad para la escalabilidad a todas las jurisdicciones.

PERSPECTIVAS DE LOS DIRECTIVOS

Las nuevas reglas de preparación

Emily Hancock
Directora de privacidad, Cloudflare

Garantizar un futuro seguro: regulación, riesgo y preparación

Las normativas de ciberseguridad están entrando en una nueva era definida por requisitos más estrictos, un mayor escrutinio y una responsabilidad más amplia. Con la obligación de la divulgación de incidentes de la SEC y las fuertes sanciones por incumplimiento en materia de privacidad del RGPD, pasando por las nuevas normas como DORA y APRA CPS 234, los organismos reguladores globales están aumentado las expectativas en torno a la protección de datos, la continuidad operativa y la transparencia. Para los equipos ejecutivos, la conformidad ya no es solo una obligación legal, sino una prioridad estratégica.

Al mismo tiempo, las nuevas tecnologías y los modelos de amenazas en evolución suponen un desafío para los enfoques tradicionales de la seguridad. A medida que se acelera la innovación, los organismos reguladores y las partes interesadas prestan más atención a la gestión de riesgos a largo plazo, especialmente en relación con los datos confidenciales. Las organizaciones deben demostrar que pueden proteger no solo sus activos actuales, sino también los datos y los sistemas que sustentarán la confianza digital del mañana.

Lo que no vemos: conceptos erróneos y vulnerabilidades que se pasan por alto

Muchas organizaciones siguen tratando la seguridad y la conformidad como funciones aisladas, gestionadas por equipos técnicos sin coordinación interdisciplinar. Esto crea puntos ciegos, especialmente en lo que respecta a comprender dónde residen los datos confidenciales, cómo se aplica la encriptación y dónde se encuentran las vulnerabilidades en los sistemas de terceros.

Sin un marco claro de inventario y gobernanza, las organizaciones corren el riesgo de quedarse rezagadas tanto respecto a los organismos reguladores como a los atacantes.

Otra vulnerabilidad es la minimización de los datos. Con demasiada frecuencia, las empresas conservan datos personales que ya no necesitan, lo que aumenta la exposición sin ningún beneficio empresarial. La incorporación de los principios de privacidad por diseño (limitar la recopilación de datos, automatizar su eliminación e incorporar controles a nivel de arquitectura) puede reducir el riesgo y mejorar la conformidad normativa.

Próximos pasos: un avance hacia la conformidad integrada

Entre los próximos 12 a 18 meses, esperamos que los organismos reguladores y de normalización pongan más énfasis en las prácticas de seguridad proactivas y verificables. Esto incluye controles más estrictos en torno a la gobernanza de datos, la encriptación y el riesgo de terceros. Las empresas que actúen pronto, mediante la adopción de plataformas integradas, la automatización de los flujos de trabajo de conformidad y la integración de la seguridad en sus operaciones principales, reducirán la complejidad, evitarán costosas medidas de corrección y se posicionarán como líderes de confianza.

El cambio es evidente: la conformidad, la continuidad y la seguridad se deben integrar por diseño desde el principio. Las organizaciones que interioricen este enfoque no solo se ajustarán a la normativa, sino que liderarán en un mundo que exige responsabilidad, transparencia y confianza.

"Sin un inventario claro y un marco de gobernanza, **las organizaciones corren el riesgo de quedarse rezagadas tanto respecto a los organismos reguladores como a los atacantes**".

4

Descifrar el código: preparar la privacidad para el futuro en la era cuántica

Descifrar el código: preparar la privacidad para el futuro en la era cuántica

La informática cuántica promete avances transformadores en la ciencia y la industria, pero también plantea una amenaza muy grave para la seguridad digital. Cuando los sistemas cuánticos a gran escala maduren, tendrán capacidad para descifrar los sistemas criptográficos de clave pública más utilizados para proteger Internet. Esto incluye la encriptación TLS, las VPN, la firma de código y los sistemas de cadena de bloques.

El peligro no es hipotético. Los ciberdelincuentes ya están recopilando datos encriptados
En la actualidad, apostando a que los futuros ordenadores cuánticos podrán descifrarlos, una estrategia conocida como "recopilar ahora, descifrar después". Ante la aceleración de la adopción de la criptografía poscuántica, los factores que definirán la preparación de la organización serán la visibilidad de los sistemas criptográficos, la aplicación automatizada de políticas y una ruta de migración clara.

Las amenazas cuánticas ya están en marcha

El Instituto Nacional de Estándares y Tecnología (NIST) ha advertido que las organizaciones deben tomar medidas ya para evitar que las pillen desprevenidas.[24] Ciberdelincuentes del estado-nación y sofisticados adversarios recopilan activamente tráfico cifrado, propiedad intelectual y secretos de estado para descifrarlos más tarde. Las comunicaciones que requieren una década (o más) de confidencialidad, como los historiales sanitarios, la inteligencia militar y los contratos legales, ya son vulnerables si no se protegen con un acuerdo de claves con resiliencia cuántica.

La adopción de la criptografía poscuántica ha aumentado, pero aún hay vulnerabilidades

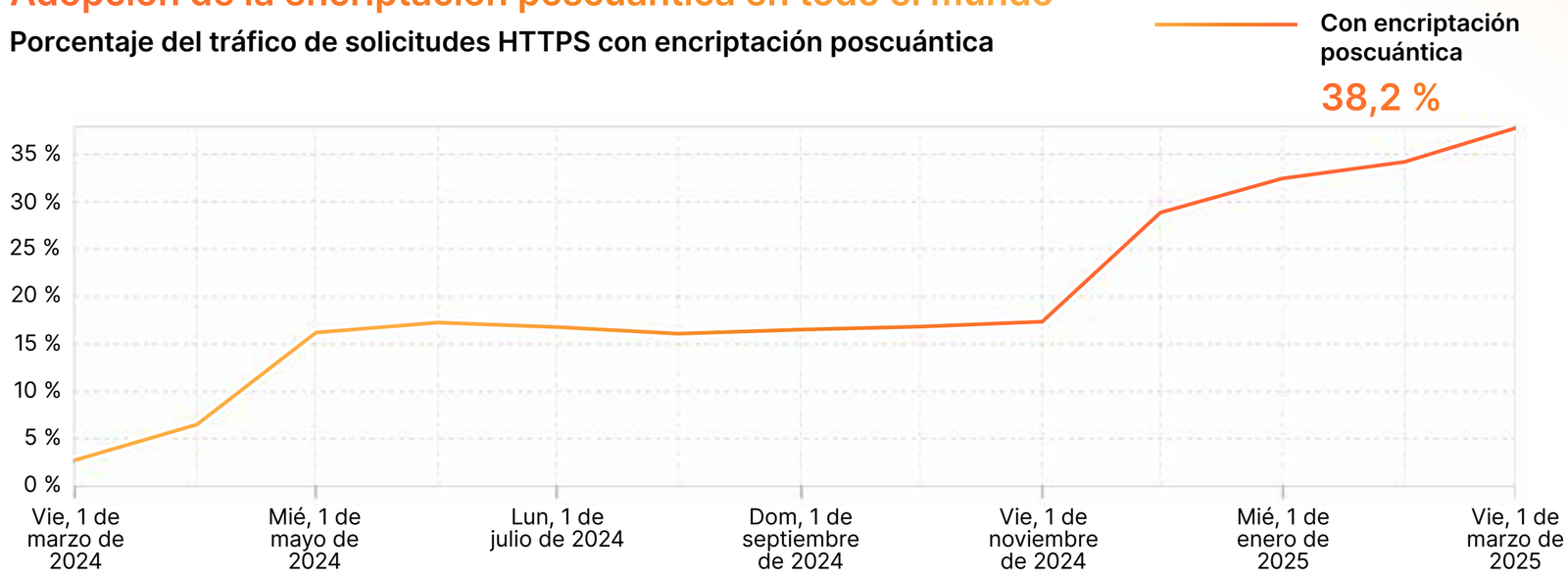
La criptografía poscuántica (PQC) ha pasado de la investigación teórica a la implementación en producción. Las principales empresas tecnológicas, como Cloudflare, están a la vanguardia en la adopción de la PQC.

A principios de 2024, Cloudflare informó de que solo el 3 % del tráfico HTTPS se encriptaba con algoritmos poscuánticos. En marzo de 2025, esa cifra alcanzó el 38 %, después de que Cloudflare implementara TLS poscuántico híbrido por defecto, y la compatibilidad de navegadores como Chrome, Edge y Firefox.[25]

Aun así, la adopción es desigual. La mayoría de los entornos empresariales se encuentran en las fases iniciales de descubrimiento o piloto, y el exceso de encriptaciones criptográficas complica la transición. Las empresas que no prioricen la encriptación a prueba de ataques cuánticos corren el riesgo de incumplir los requisitos normativos y de exponer sus datos a vulnerabilidades a largo plazo.

Adopción de la encriptación poscuántica en todo el mundo

Porcentaje del tráfico de solicitudes HTTPS con encriptación poscuántica



Estrategia para la migración cuántica

1

Empieza por documentar todos los lugares en los que se utiliza la criptografía.

Crea una lista de proyectos de migración, priorizados según el riesgo y el nivel de esfuerzo.

2

Integra ya la preparación poscuántica en tu proceso de evaluación de proveedores.

No todos los proveedores son iguales a la hora de adoptar los últimos estándares. Valida la criptoagilidad de los proveedores, especialmente tus proveedores Zero Trust que tunelizan el tráfico de la red corporativa.

3

Prioriza primero las migraciones de acuerdos de claves.

Debido a la amenaza de la táctica de tipo "recopilar ahora, descifrar después", garantizar que tu acuerdo de claves sea resistente ahora a la computación cuántica ofrece una clara ventaja. Los proveedores han coincidido en gran medida en la transición de TLS 1.3 para la compatibilidad con X25519MLKEM768: un híbrido del algoritmo criptográfico X25519 de curva elíptica convencional junto con el algoritmo ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203) poscuántico.

4

Las migraciones de firmas se deben documentar pero no es necesario priorizarlas en este momento.

Las organizaciones siguen trabajando para llegar a un consenso sobre el enfoque adecuado para migrar a las firmas poscuánticas. Afortunadamente, las firmas poscuánticas protegen principalmente contra los ataques en ruta activos, lo que hace que esta migración tenga menos prioridad.

La visibilidad criptográfica y la automatización basada en XDR acelerarán la transición

La migración poscuántica no consiste únicamente en implementar los nuevos algoritmos, sino en comprender dónde se encuentra la criptografía en los entornos en expansión. Esto incluye los sistemas integrados, las cargas de trabajo en la nube, las aplicaciones heredadas, las API y los dispositivos IoT. Los equipos de seguridad que utilizan plataformas de detección y respuesta extendidas (XDR) con telemetría de red profunda y de punto final están mejor posicionados para identificar la criptografía obsoleta, detectar comportamientos alternativos inseguros y automatizar los flujos de trabajo de corrección.

La criptoagilidad de los proveedores será un factor diferenciador a nivel de riesgo

Los organismos reguladores (p. ej., NIST, BSI, ANSSI) están empezando a recomendar o exigir arquitecturas criptoágiles. Las empresas evaluarán cada vez más la preparación poscuántica en los procesos de solicitudes de propuestas y en las auditorías de la cadena de suministro. Sin embargo, no todos los proveedores avanzan al mismo ritmo. Aquellos que no admitan la encriptación híbrida o a prueba de las amenazas cuánticas pueden verse descalificados, especialmente en los sectores de los servicios gubernamentales, financieros y de defensa.

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Prepararse para los riesgos cuánticos

A medida que los atacantes adoptan la táctica de tipo "recopilar ahora, descifrar después" y los organismos reguladores avanzan hacia los requisitos poscuánticos, las organizaciones deben empezar a prepararse hoy mismo. Los ejecutivos que lideren esta transición no solo prepararán su infraestructura para el futuro. También se beneficiarán de una ventaja estratégica en términos de confianza, conformidad y resiliencia. **Analiza tu preparación para la inminente era de los riesgos cuánticos planteándote estas preguntas:**

P1

¿Tenemos visibilidad integral de dónde se utiliza la criptografía en nuestro entorno, desde las nubes y las aplicaciones hasta los sistemas integrados y las herramientas de terceros?

Los sistemas criptográficos suelen estar profundamente integrados e insuficientemente documentados. Sin una visibilidad integral, las organizaciones corren el riesgo de dejar los sistemas críticos desprotegidos o expuestos sin saberlo a las amenazas de la era cuántica.

P2

¿Hemos priorizado la migración a protocolos de acuerdo de claves poscuánticos, especialmente para los sistemas que protegen datos confidenciales o de larga duración?

Los ataques de tipo "recopilar ahora, descifrar después" tienen como objetivo datos que deben seguir siendo confidenciales durante años. La migración de los mecanismos de intercambio de claves, como los protocolos de enlace TLS, es una medida urgente y efectiva para garantizar la confidencialidad en el futuro.

P2

¿Nuestras herramientas de detección y supervisión de activos pueden identificar la criptografía obsoleta o vulnerable a la computación cuántica en toda la empresa?

Las plataformas XDR, SIEM y de descubrimiento de activos deberían ayudar a detectar la desviación criptográfica, las bibliotecas heredadas y los protocolos de reserva. Esto es esencial para evitar errores de configuración y orientar sobre las prioridades de la migración.

P4

¿Evaluamos la criptoagilidad de nuestros proveedores y socios como parte de nuestro proceso de compras y de revisión de riesgos?

Los proveedores que carecen de una hoja de ruta para la preparación poscuántica pueden llegar a ser puntos débiles. La incorporación de la alineación con la PQC en las medidas oportunas ayuda a reducir la exposición de los recursos descendentes y garantiza la resiliencia a largo plazo.

P5

¿Tenemos una estrategia de migración por fases, basada en el riesgo, que incluya la gobernanza, la automatización y la visibilidad ejecutiva?

La migración poscuántica es un proceso complejo que lleva varios años. Una hoja de ruta clara que incluya responsabilidad, automatización de la implementación y métricas en tiempo real del progreso es imprescindible para mantener el impulso y la confianza del consejo de administración.

PERSPECTIVAS DE LOS DIRECTIVOS

Evitar la confusión criptográfica

Wesley Evans
Director sénior de producto, Cloudflare

Las organizaciones afrontan un aumento de la complejidad criptográfica. Donde antes teníamos unas pocas normas bien definidas, ahora tenemos un ecosistema fragmentado de algoritmos y modelos de implementación. Esta rápida evolución, junto con la creciente presión normativa y operativa para adoptar la encriptación a prueba de la informática cuántica, ha generado confusión en las empresas.

Se pide a los directivos que adopten la criptoagilidad y que se preparen para la resiliencia cuántica, pero la mayoría de ellos carece de un inventario claro de dónde y cómo se utiliza la criptografía. Sin visibilidad, la planificación no deja de ser más que conjeturas. El presupuesto se paraliza. La propiedad no está clara. Y eso facilita que los ejecutivos resten prioridad a la medida, incluso comprendiendo bien los riesgos.

Errores comunes

Un punto ciego importante es la suposición de que las organizaciones aún no han estado en riesgo. Los ataques de tipo "recopilar ahora, descifrar luego" son reales y activos, especialmente para los datos con un valor a largo plazo, como los registros médicos, la propiedad intelectual y la información de seguridad nacional. Si tus datos corresponden a estas categorías, es posible que ya estén en manos de un ciberdelincuente a la espera de que pueda descifrarlos.

Otra idea errónea es que el riesgo cuántico irá precedido por un hito claro, como un avance público en el algoritmo de Shor. Sin embargo, los atacantes no necesitan resultados instantáneos.

Si les lleva semanas o incluso meses descifrar una clave pero la recompensa es suficientemente significativa, se dedicarán a esa tarea. Este retraso en la percepción contribuye a una peligrosa sensación de complacencia.

Orientación futura

Se avecinan dos cambios. En primer lugar, los avances en la corrección de errores cuánticos harán que la amenaza del descifrado cuántico parezca real, no teórica. Esto llevará a una mayor presión por parte de los organismos reguladores, los consejos de administración y el público. En segundo lugar, las organizaciones empezarán a implementar sistemas criptoágiles. Es decir, finalmente harán un balance de dónde se encuentra la criptografía, cómo se utiliza y quién es su propietario.

No será fácil. La mayoría de los equipos afrontan esta situación como una visita al dentista criptográfico que deberían haber hecho hace mucho tiempo, y que conlleva molestias, costes y sorpresas. Sin embargo, postergarlo solo empeora la situación. La prioridad ahora no es reemplazar todo de la noche a la mañana, sino mejorar la visibilidad, asignar responsabilidades e iniciar la ruta de actualización. Los que actúen pronto estarán mejor posicionados para gestionar el cambio poscuántico, antes de que se convierta en una crisis.

"Los avances en la corrección de errores cuánticos harán que la **amenaza del descifrado cuántico** parezca real, no teórica".

5

Cambiar la balanza: gobernanza, geopolítica y ética

Cambiar la balanza: gobernanza, geopolítica y ética

A medida que cambia la dinámica del poder global, la intersección de la ciberseguridad, la geopolítica y la ética está redefiniendo las responsabilidades de los líderes. Hoy en día, los ciberataques son herramientas de influencia geopolítica, los organismos reguladores exigen responsabilidades personales a los ejecutivos, y la IA plantea dilemas éticos que desafían la supervisión tradicional.

Con cambios como el requisito de la SEC de 2023 de divulgar rápidamente los incidentes de ciberseguridad y los informes generalizados de ciberoperaciones patrocinadas por estados, los líderes empresariales deben integrar en su estrategia una gobernanza eficaz, una ética transparente de la IA y una gestión ágil de los riesgos.

La gobernanza de la seguridad pasa de la orientación a la responsabilidad

La supervisión normativa es cada vez más estricta. En 2023, la SEC ordenó a las empresas públicas que revelaran los incidentes de ciberseguridad en un plazo de cuatro días, lo que marcó un cambio hacia la obligación de exigir responsabilidades. Ahora, casi el 72 % de las empresas priorizan los conocimientos en ciberseguridad en sus consejos de administración, y el 71 % la incluye en al menos la biografía de un director, frente a solo el 34 % en 2018.[26] Los consejos de administración reconocen cada vez más que descuidar la ciberseguridad puede generar graves problemas operativos, legales y de daños a la reputación.

La geopolítica y la guerra cibernética afectan directamente a la empresa

Los ciberdelincuentes del estado-nación y los grupos hacktivistas utilizan cada vez más las ciberoperaciones como armas estratégicas. En los últimos años, se han lanzado campañas respaldadas por estados contra los sectores financiero, energético y tecnológico con el objetivo de interrumpir las cadenas de suministro globales e influir en la dinámica del mercado. Por ejemplo, LameDuck, un grupo de ciberdelincuentes con motivaciones políticas, llevó a cabo más de 35 000 ataques DDoS confirmados en el plazo de un año, que causaron la interrupción operativa de organizaciones como Microsoft, OpenAI y Scandinavian Airlines.[27] Incluso las organizaciones aparentemente neutrales pueden verse envueltas en conflictos geopolíticos.

Los ejecutivos deben considerarse superficies de ataque

Los equipos directivos afrontan ciberamenazas directas. Las estafas deepfake de gran repercusión y las estrategias de suplantación de ejecutivos han aumentado exponencialmente, y varios directores generales han sido objetivo de mensajes de audio y vídeo fraudulentos diseñados para engañar a las partes interesadas.[28]

Estos incidentes subrayan la gran vulnerabilidad de la directiva ante los riesgos de ciberseguridad y los ataques de tipo económico y a la reputación.

Aumento de la fragmentación normativa y de la incertidumbre de la cadena de suministro

Las empresas globales afrontan ahora un laberinto de leyes divergentes en materia de ciberseguridad, IA y soberanía de datos. Las restricciones comerciales y los controles de la exportación han obligado a las empresas a reevaluar las relaciones con sus proveedores y a reconfigurar las cadenas de suministro. Por ejemplo, los cambios en los aranceles y la directiva NIS2 de la UE han interrumpido los protocolos establecidos de la cadena de suministro. Esto ha incrementado tanto los costes relacionados con el cumplimiento normativo como el riesgo de retrasos operativos.

La ética de la IA y la Shadow AI exigen la gobernanza a gran escala

El auge de la IA generativa en el lugar de trabajo está superando el control de las organizaciones. McKinsey informa de que el 65 % de las empresas utilizan ahora la IA generativa en al menos una función empresarial, frente a un tercio en 2023.[29] AI Gateway de Cloudflare procesó más de 5000 millones de solicitudes entre octubre de 2024 y febrero de 2025, lo que supone un aumento del 60 % en solo cinco meses.[30] La adopción es extremadamente rápida: en enero de 2025, DeepSeek AI alcanzó el tercer puesto en la lista de servicios de IA de Cloudflare Radar a los nueve días del lanzamiento de su modelo R1.[31]

Esta adopción generalizada está impulsando el auge de la Shadow AI, es decir, las herramientas no autorizadas que utilizan los empleados sin supervisión. Estas herramientas plantean graves riesgos: la fuga de datos, el incumplimiento normativo y la exposición de información confidencial a modelos públicos.

Para abordar este problema, las organizaciones deben ir más allá de las declaraciones de políticas básicas. Una gobernanza eficaz requiere marcos de aprobación claros, el registro de instrucciones, el filtrado de URL y la supervisión del uso. Sin la aplicación activa de estas funciones, la ética y la seguridad de la IA seguirán siendo teóricas.

> Los ciberdelincuentes del estado-nación y los grupos hacktivistas utilizan cada vez más las ciberoperaciones como **armas estratégicas**.

PREGUNTAS PARA EL EQUIPO DIRECTIVO

Sortear el riesgo ético y geopolítico

Ante la dependencia de las ciberamenazas de factores geopolíticos, la creciente complejidad de la ética de la IA y las mayores expectativas normativas, los equipos ejecutivos deben ir más allá de los controles técnicos. **Estas preguntas pueden ayudar a los líderes empresariales a evaluar si sus estrategias de gobernanza, información y respuesta son adecuadas para un mundo en el que los propios directivos forman parte de la superficie de amenazas.**

P1

¿Están claramente establecidas las responsabilidades a nivel de consejo de administración en materia de seguridad y resiliencia digital, con funciones bien definidas y un equipo directivo con conocimientos sobre ciberseguridad?

Dado que los organismos reguladores ahora responsabilizan personalmente a los ejecutivos, como hemos visto con los requisitos de divulgación rápida de la SEC, es fundamental garantizar que el equipo directivo cuente con conocimientos específicos en ciberseguridad para mitigar los riesgos legales y para la reputación.

P2

¿Supervisamos los cambios geopolíticos y su impacto en nuestro panorama de amenazas, como los ciberataques patrocinados por estados y las campañas de activistas?

Las recientes operaciones respaldadas por estados contra sectores críticos del mercado han interrumpido las cadenas de suministro. Por lo tanto, es imprescindible disponer de información en tiempo real sobre el riesgo geopolítico para proteger tanto las operaciones globales como a los directivos.

P3

¿Tenemos un plan de respuesta proactivo para los ataques contra ejecutivos, como las estafas deepfake y las campañas de suplantación de identidad?

Los directivos afrontan riesgos cada vez mayores derivados de la desinformación y la suplantación de identidad impulsadas por la IA, y las estrategias de respuesta deben incluir protocolos de respuesta a incidentes específicos y medidas continuas de gestión de la reputación.

P4

¿Nuestras políticas y nuestros controles de seguridad son lo suficientemente eficaces como para detectar y gestionar el uso no autorizado de la IA por parte de nuestros usuarios?

El uso cada vez más generalizado de la IA generativa por parte de las organizaciones y el incremento del uso de la Shadow AI requieren un control granular y la aplicación de directrices estrictas para evitar las fugas de datos y garantizar la conformidad normativa.

P5

¿Adaptamos nuestras estrategias de ciberseguridad e IA a la evolución de la normativa regional en materia de soberanía de los datos e IA ética? ¿Utilizamos esta alineación como una ventaja estratégica?

Los marcos normativos divergentes, como la directiva NIS2 de la UE y las leyes regionales en materia de soberanía de datos, exigen que las políticas de seguridad sean ágiles y con visión de futuro. Esta alineación reduce el riesgo legal y mejora la confianza del mercado y el posicionamiento competitivo.

PERSPECTIVAS EJECUTIVAS

Gobernanza y responsabilidad en un mundo en policrisis

Ramy Houssaini
Director de soluciones de ciberseguridad, Cloudflare

Las organizaciones deben sortear un panorama de policrisis en el que se entrecruzan los riesgos geopolíticos, económicos y tecnológicos. El requisito de divulgación de incidentes de ciberseguridad de la SEC ejemplifica el cambio de orientación de la ciberseguridad a la responsabilidad de la ejecutiva. Las organizaciones deben desarrollar capacidades de detección y respuesta a las fugas en tiempo real. El incumplimiento conlleva graves sanciones, mientras que el daño a la reputación puede erosionar la confianza de las partes interesadas. Para garantizar la resiliencia, los consejos de administración deben incorporar conocimientos en ciberseguridad y la gestión proactiva de riesgos.

Puntos ciegos: riesgos geopolíticos, de la IA y de la cadena de suministro

Uno de los principales puntos ciegos es subestimar las ciberamenazas geopolíticas. Muchas empresas se declaran neutrales, pero los ataques patrocinados por estados perturban cada vez más los sectores financiero, tecnológico y energético, exponiendo las cadenas de suministro.

Otro riesgo que se pasa por alto es la Shadow AI, es decir, las herramientas de IA no autorizadas que se utilizan sin supervisión. Sin un control eficaz, los datos confidenciales pueden quedar expuestos, con las consiguientes sanciones por incumplimiento de las normativas y desventajas competitivas.

Además, los proveedores externos (y sus propios proveedores) abren la puerta a vulnerabilidades ocultas. Aunque las empresas se centran en los proveedores directos, los extensos ecosistemas de proveedores suelen carecer de visibilidad, por lo que son susceptibles a las ciberamenazas y a las interrupciones operativas.

Preparación estratégica y avances futuros

Entre los próximos 12 y 18 meses, las organizaciones pueden prever:

- **La ampliación de la normativa:** la directiva NIS2 de la UE y marcos similares aumentarán los requisitos relacionados con el cumplimiento normativo. Para anticiparse, los líderes empresariales deben establecer grupos de trabajo en materia de normativa.
- **La aceleración de la gobernanza de la IA:** con el auge de la Shadow AI, los organismos reguladores impondrán controles más estrictos. Para mitigar los riesgos, las empresas deben aplicar marcos de supervisión y gobernanza.
- **Ataques a ejecutivos:** las estafas deepfake y los ataques de suplantación de identidad serán cada vez más sofisticados, lo que aumentará los riesgos de fraude y desinformación. Las organizaciones deben implementar sistemas de detección basados en IA y mejorar la formación en seguridad del equipo ejecutivo.
- **Resiliencia de la cadena de suministro:** las ciberamenazas y la inestabilidad geopolítica seguirán afectando a las cadenas de suministro. Las empresas deben reforzar las evaluaciones de riesgos, aplicar obligaciones en materia de seguridad y mejorar la supervisión de los proveedores.

Para tener éxito en esta era de policrisis, los líderes empresariales deben integrar la ciberseguridad en la gobernanza, evaluar los riesgos geopolíticos, aplicar la supervisión de la IA y desarrollar cadenas de suministro resilientes. La agilidad y una mejor gestión de riesgos serán fundamentales para sortear los cambios de las normativas y garantizar la estabilidad a largo plazo.

"Para garantizar la resiliencia, los consejos de administración deben **incorporar conocimientos en ciberseguridad y la gestión proactiva de riesgos**".

CONCLUSIÓN

Avances de los equipos directivos que mejoran la resiliencia a gran escala

La naturaleza de la ciberseguridad ha cambiado: ahora afecta a todas las áreas de la empresa. En 2025, los ataques basados en la IA, el riesgo geopolítico, la complejidad normativa y las interdependencias de la cadena de suministro exigen una respuesta coordinada e interdisciplinar. Para garantizar un futuro seguro es necesario algo más que reaccionar ante las amenazas. Requiere integrar la resiliencia en las estrategias operativas, de innovación y de crecimiento de las organizaciones. Estas llamadas a la acción están diseñadas para que los equipos ejecutivos mejoren la resiliencia como una capacidad estratégica, juntos.

1 Resiliencia: un requisito estratégico compartido

Mejora la propiedad interdisciplinar de la ciberseguridad garantizando que todo el equipo directivo tenga una visión unificada en cuanto a la postura de seguridad, la asignación de recursos y la planificación de contingencias. La resiliencia no es responsabilidad de un único equipo. Es una capacidad empresarial que debe escalarse a todas las funciones y zonas geográficas.

2 Automatización e integración para garantizar la escalabilidad

La conformidad manual y las soluciones de seguridad fragmentadas no pueden adaptarse a los cambios de las amenazas de la IA y de los requisitos normativos en expansión. Invierte en automatización para la detección de amenazas, los flujos de trabajo de conformidad y la respuesta a incidentes. Integra las herramientas de conformidad, riesgos y seguridad para eliminar los silos y mejorar la visibilidad.

3 Replantear la cibergobernanza como una ventaja competitiva

Ante la mayor responsabilidad que recae sobre la ejecutiva, garantiza que tu consejo de administración y tu equipo directivo tengan conocimientos sobre ciberseguridad y funciones formalizadas para la supervisión de los riesgos digitales. Integra el ciberriesgo en los marcos de riesgo empresarial y considera la alineación normativa como un elemento diferenciador competitivo.

4 Prepararse para el futuro ahora, no más adelante

Empieza hoy mismo tu migración a la criptografía poscuántica (PQC) y la preparación para la gobernanza de la IA. Los responsables empresariales que lo pospongan quedarán expuestos a las amenazas de tipo "recopilar ahora, descifrar después" o a la expansión descontrolada de la IA. La visibilidad, la criptoagilidad de los proveedores y las estrategias de migración por fases son fundamentales.

5 Prueba de fallos a gran escala

La resiliencia no consiste en evitar los fallos, sino en seguir funcionando a pesar de ellos. Simula crisis reales, desde ataques DDoS hipervolumétricos al uso indebido de información privilegiada o ataques contra los ejecutivos, y prueba tu capacidad de detección, contención y recuperación. Considera la conformidad, las comunicaciones y la cadena de suministro en tus escenarios.

6 Integración de la IA en la defensa y la ofensiva

La IA debe dejar de considerarse solo como una herramienta. Se trata una capacidad estratégica del equipo directivo, que mejora la agilidad, la resiliencia y la innovación en toda la empresa. Con la información que proporciona la IA, las organizaciones pueden adaptarse rápidamente a los cambios del mercado, prever los riesgos y optimizar la toma de decisiones en tiempo real.

La IA mejora la resiliencia al automatizar la detección de amenazas, agilizar la respuesta a las crisis y reforzar las posturas de ciberseguridad contra los riesgos en constante cambio. Además, impulsa la innovación al identificar nuevas fuentes de ingresos, acelerar el I+D y personalizar las experiencias de los clientes a gran escala. Cuando las organizaciones integran plenamente la IA en sus funciones empresariales básicas, se transforman en empresas preparadas para el futuro y con mayor capacidad de adaptación, así que los líderes empresariales pueden abordar la complejidad con confianza.

Para garantizar un futuro seguro es necesario algo más que reaccionar ante las amenazas. **Requiere integrar la resiliencia en las estrategias operativas, de innovación y de crecimiento de las organizaciones.**

Estas llamadas a la acción están diseñadas para que los equipos ejecutivos **mejoren la resiliencia como una capacidad estratégica, juntos.**

La resiliencia en Cloudflare: las bases para un futuro más escalable

LA RESILIENCIA EN CLOUDFLARE

Una red única y programable como ninguna otra

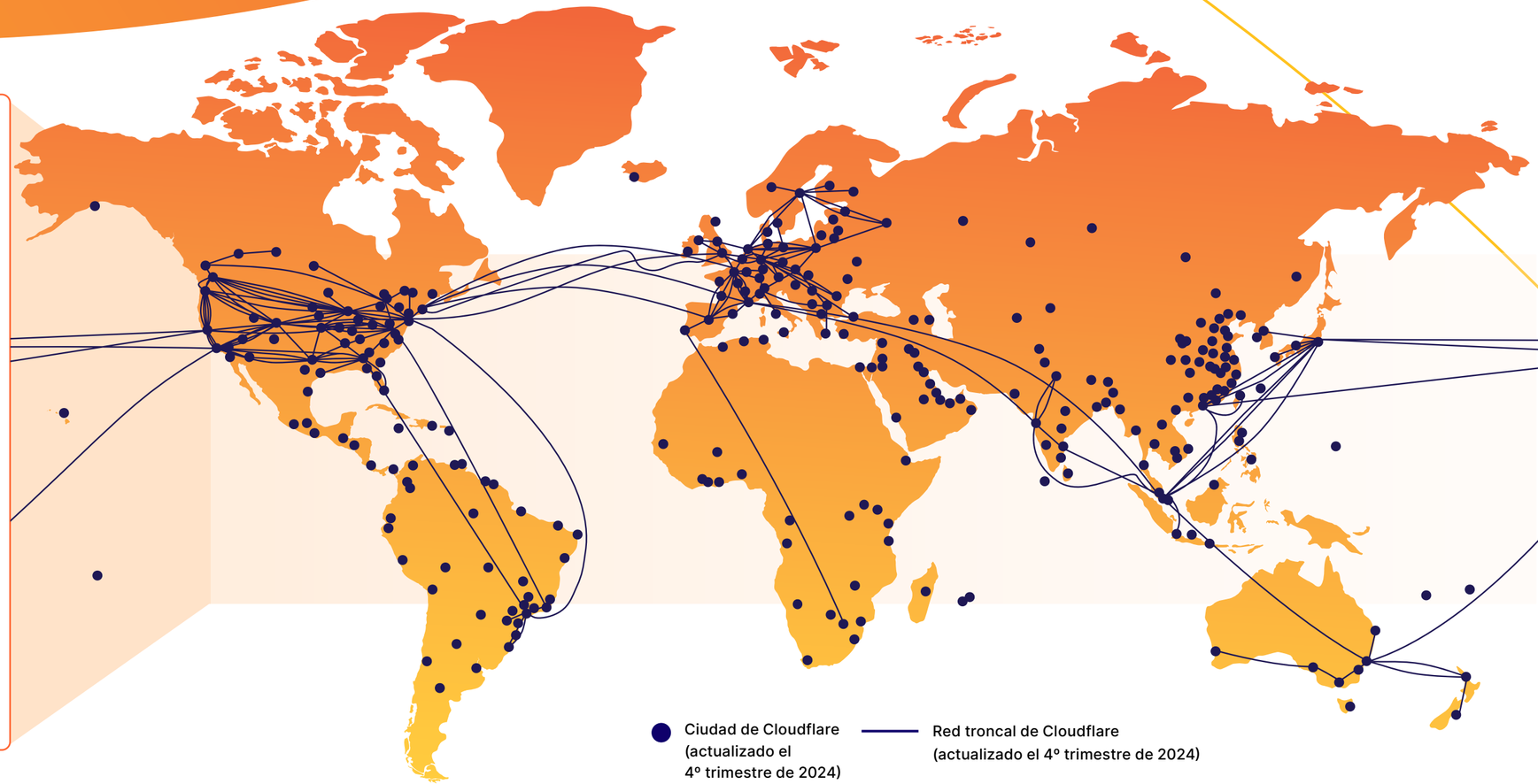
Más de 335 ciudades
en más de 125 países, incluida China continental

↳ **con +190 ciudades**
para la inferencia de IA con tecnología de GPU

~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 servicios de Internet, proveedores de nube y grandes empresas

348 Tb/s
de capacidad de red (y continúa creciendo)



LA RESILIENCIA EN CLOUDFLARE

Cloudflare Workers

La mejor plataforma para que los desarrolladores creen y escalen la inferencia y los agentes de IA

Coste y escalabilidad

Escala según sea necesario

Ejecuta modelos de IA en GPU sin tener que pagar por recursos aprovisionados previamente con meses de antelación, en los momentos de mayor demanda. Simplemente paga por lo que usas.

Sin procesos = sin facturas por uso

Los precios basados en procesos significan que no se te cobrará cuando tu función esté esperando E/S. (Las aplicaciones pueden pasar **diez veces** más tiempo esperando E/S que utilizando la CPU).

Rendimiento

Implementación en cualquier lugar del mundo

El código se ejecuta a menos de 50 ms de aproximadamente el 95 % de la población mundial conectada a Internet.

Orquestación y ejecución en un solo lugar

Workers puede interactuar con las API, los LLM y los servicios externos o internos, dondequiera que sea más eficiente su ejecución.

Experiencia del desarrollador

Todos los productos que necesitas

Accede a la inferencia, la gestión de estado, la implementación de la interfaz de usuario o los flujos de trabajo en una sola plataforma.

De la idea a la producción en cuestión de segundos

Experiencia de desarrollo sencilla, que incluye el desarrollo local y una implementación rápida.

Ahorra tiempo

No es necesario realizar ajustes. Ubicación automática para un rendimiento óptimo.

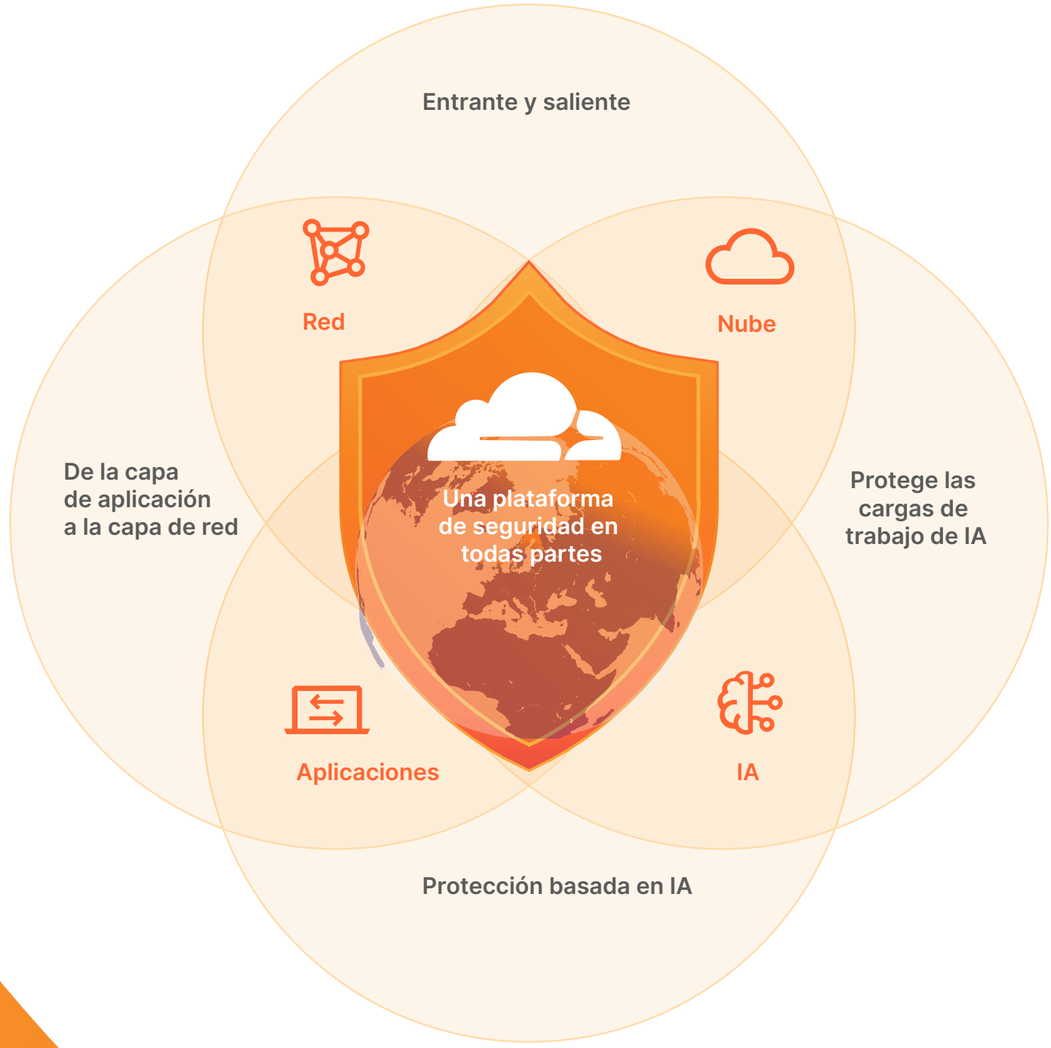
Tú escribes el código. Nosotros nos encargamos del resto.

LA RESILIENCIA EN CLOUDFLARE

Una plataforma de seguridad. De la red a la nube. De las aplicaciones a la IA.

Permite a las organizaciones:

- Recuperar el control operativo
- Mejorar la postura de seguridad
- Acelerar la consolidación de proveedores
- Mejorar la experiencia del usuario y la productividad
- Lograr la gobernanza de datos y el cumplimiento normativo



LA RESILIENCIA EN CLOUDFLARE

Cloudflare se ha desarrollado para afrontar los desafíos del futuro

Una plataforma componible

Seguridad unificada

para sistemas externos y recursos internos

Una conectividad universal

para usuarios, aplicaciones, filiales, centros de datos y nubes

Flexibilidad

para personalizar la plataforma con herramientas integrales para desarrolladores

Una red programable

Más eficaz

ya que simplifica la conectividad y la gestión de políticas.

Más productiva

ya que garantiza experiencias de usuario rápidas, fiables y coherentes en todas partes.

Más ágil

gracias a su capacidad para innovar rápidamente y satisfacer los requisitos de seguridad en constante evolución.

LA RESILIENCIA EN CLOUDFLARE

Ejecuta tareas de inferencia en Workers AI, la primera plataforma de inferencia de IA sin servidor distribuida globalmente

Implementación en cualquier lugar del mundo

+335 ciudades

en más de 125 países, incluida China continental

El código se ejecuta a menos de 50 ms de aproximadamente el 95 % de la población mundial conectada a Internet

+190 ciudades

con GPU

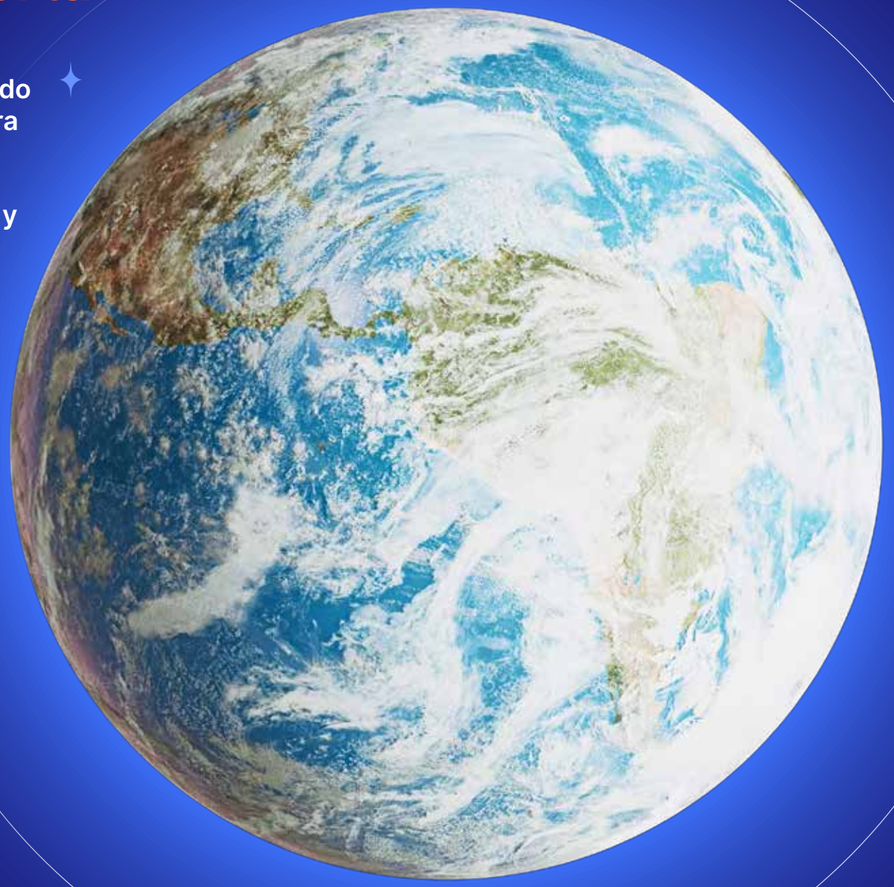
Un conjunto cada vez mayor de ciudades para la inferencia de IA basada en GPU

LA RESILIENCIA EN CLOUDFLARE

Luchar por una Internet abierta

Internet es un milagro. La conexión de diversas redes con estándares comunes nos permite intercambiar datos en todo el mundo de forma resiliente, interoperable y accesible para todos. Hoy en día, dependemos de ella para el crecimiento económico y la innovación, el acceso a la información y la libertad de expresión, así como para el Estado de Derecho y los principios democráticos.

Cloudflare se enorgullece de formar parte de la comunidad global que defiende Internet.



- Defensa de la neutralidad de la red
- Supervisión de lugares donde Internet no está abierto
- Protección de los derechos humanos y de las instituciones democráticas
- Implementación de normas que mejoran la privacidad y la seguridad de los flujos de datos
- Participación en la elaboración de normas de Internet
- Respaldo de la gobernanza multilateral de Internet

CLOUDFLARE

2025

Informe Cloudflare Signals

Más información

Resiliencia a gran escala

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

REV:BDES-6966.24ABR2025

Notas finales

Las conclusiones de este informe se han obtenido principalmente de los patrones de tráfico agregado observados en la red global de Cloudflare entre el 2 de enero de 2024 y el 31 de diciembre de 2024.

1. https://www.darktrace.com/blog/survey-findings-ai-cyber-threats-are-a-reality-the-people-are-acting-now/
2. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
3. Análisis de Cloudflare Radar, 2024
4. https://www.cnbc.com/2025/02/24/chegg-sues-google-for-hurting-traffic-as-it-considers-alternatives.html; https://www.theguardian.com/gnm-press-office/2025/feb/25/make-it-fair
5. Análisis de Cloudflare Radar, 2024
6. https://nationalcioreview.com/wp-content/uploads/2024/07/2023_Insider_Threat_Report-16d8d8f7.pdf
7. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
8. https://www.verizon.com/business/resources/T1e3/reports/2024-dbir-data-breach-investigations-report.pdf
9. Análisis de Cloudflare Radar, 2024. https://radar.cloudflare.com/bots
10. https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/; https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
11. Análisis de Cloudflare Radar, 2024
12. Análisis de Cloudflare Radar, 2024
13. https://blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/
14. https://therecord.media/advance-auto-parts-data-breach-2million
15. Análisis de Cloudflare Radar, del 12 de octubre de 2024 al 31 de diciembre de 2024
16. Análisis de Cloudflare Radar, del 12 de octubre de 2024 al 31 de diciembre de 2024. https://radar.cloudflare.com/security/application-layer
17. Análisis de Cloudflare Radar, 2024. https://blog.cloudflare.com/tag/ddos-reports/
18. Análisis de Cloudflare Radar, 2024. https://radar.cloudflare.com/reports/ddos-2024-q4
19. https://reports.weforum.org/docs/WEF_Global_Cyber security_Outlook_2025.pdf
20. https://www.verizon.com/business/resources/Tdd6/reports/2024-dbir-data-breach-investigations-report.pdf
21. Análisis de Cloudflare Radar, 2024
22. https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf
23. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-survey-findings-on-esg-disclosure-and-preparedness.pdf
24. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
25. Análisis de Cloudflare Radar, 2024. https://radar.cloudflare.com/adoption-and-usage
26. https://www.ey.com/en_us/board-matters/cyber-disclosure-trends
27. https://www.cloudflare.com/threat-intelligence/research/report/inside-lameduck-analyzing-anonymous-sudans-threat-operations/
28. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam
29. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024
30. Análisis de Cloudflare Radar, de octubre de 2024 a febrero de 2025
31. Análisis de Cloudflare Radar, enero de 2025. https://radar.cloudflare.com/ai-insights