Softtek®

Cybersecurity Reinvented

Una nueva realidad digital abre el camino a una nueva forma de entender la ciberseguridad

Por qué la ciberseguridad ha cambiado fundamentalmente

Durante años, la ciberseguridad se ha construido sobre un conjunto de supuestos que, en su momento, permitieron proteger los sistemas, contener los incidentes y gestionar el riesgo de manera razonablemente eficaz. En aquel entonces, el entorno digital era más limitado, los ataques eran más esporádicos y el tiempo jugaba a favor del defensor. Sin embargo, **en tan solo unos pocos años, ese equilibrio se ha roto de forma irreversible**.

La aceleración del entorno digital, impulsada por la **adopción masiva de la nube, la hiperconectividad de los ecosistemas empresariales y, de manera especialmente disruptiva, por la inteligencia artificial**, ha transformado la naturaleza del riesgo. Ya no nos enfrentamos a una evolución incremental del panorama de amenazas, sino a una realidad cualitativamente diferente, en la que muchos de los supuestos que sustentaban los modelos tradicionales de ciberseguridad han dejado de ser válidos.

Fuentes: Cisco | World Economic Forum | Blackberry

Uno de los cambios más profundos es la transformación del propio ataque

La inteligencia artificial, y en particular la IA generativa, no solo amplía la superficie de ataque, sino que elimina fricciones que antes limitaban la escala, la velocidad y la persistencia del adversario. El resultado es un entorno de exposición permanente, en el que el riesgo deja de ser un evento puntual para integrarse en el funcionamiento normal del negocio.

Es así como nace el punto de inflexión, **la ciberseguridad ya no protege frente a incidentes, sino que debe operar en un contexto donde el ataque es continuo, automatizado y adaptativo**. Este cambio se refleja con claridad en los dominios que las organizaciones identifican como más difíciles de proteger: identidad, red, *cloud* y dispositivos. No se trata de áreas nuevas, sino del núcleo del ecosistema digital actual, donde confluyen usuarios, datos, infraestructuras distribuidas y, cada vez más, capacidades de inteligencia artificial.

En estos dominios, **la superficie de ataque y la complejidad operativa crecen de forma simultánea**, haciendo insuficientes los enfoques basados en controles estáticos, segmentación tradicional o confianza implícita.

Áreas que las empresas consideran más difíciles de proteger frente a nuevos ciberataques

- 31% RED
- 29% IDENTIDAD
- 16% NUBE
- 15% DISPOSITIVOS
- 10% IA *WORKLOADS*

Fuentes: Cisco | World Economic Forum | Blackberry

La complejidad sistémica amplifica los riesgos en todo el ecosistema digital

A esta presión estructural se suma la **convergencia de factores que amplifican la complejidad del entorno**: tensiones geopolíticas crecientes, cadenas de suministro digitales cada vez más interdependientes y opacas, y una adopción acelerada de tecnologías emergentes que introduce nuevas dependencias y vulnerabilidades.

El riesgo ya no se concentra dentro de los límites de la organización, sino que **se propaga a través de ecosistemas distribuidos**, donde un fallo externo puede tener un impacto directo sobre la continuidad del negocio.

Factores que agravan la complejidad de la nueva ciberseguridad

La nueva realidad

Tensiones geopolíticas

La normalización del ciberconflicto introduce ataques persistentes y tolerantes al riesgo, desbordando modelos defensivos diseñados para incidentes puntuales

Sofisticación del *cybercrime*

El cibercrimen se ha industrializado, operando con modelos eficientes, automatizados y continuos frente a defensas aún reactivas y fragmentadas

Interdependencias de la *supply chain*

La dependencia de terceros amplía el perímetro más allá del control directo, permitiendo al adversario escalar impactos a través de un único punto débil

Brecha de competencias digitales

La escasez de talento convierte la dependencia de procesos humanos en una desventaja estructural frente a adversarios automatizados que operan sin fatiga, a escala y en tiempo continuo

IA y tecnologías emergentes

La IA acelera el ataque más rápido de lo que las organizaciones la integran en la defensa, rompiendo el equilibrio entre detección, decisión y respuesta

Requisitos normativos

El cumplimiento aumenta la carga operativa, pero no garantiza control real, creando una brecha entre seguridad documentada y capacidad efectiva que el adversario explota

La presión regulatoria pone de manifiesto los límites de los modelos tradicionales de ejecución de la ciberseguridad

La regulación se ha convertido en uno de los principales catalizadores del nuevo paradigma de ciberseguridad, forzando a las organizaciones a integrar la seguridad, la resiliencia y la responsabilidad en los mecanismos de gobierno corporativo y toma de decisiones. **Los nuevos marcos normativos no solo exigen controles técnicos, sino capacidad real de operar bajo riesgo**, continuidad del negocio, gestión de terceros y responsabilidad ejecutiva.

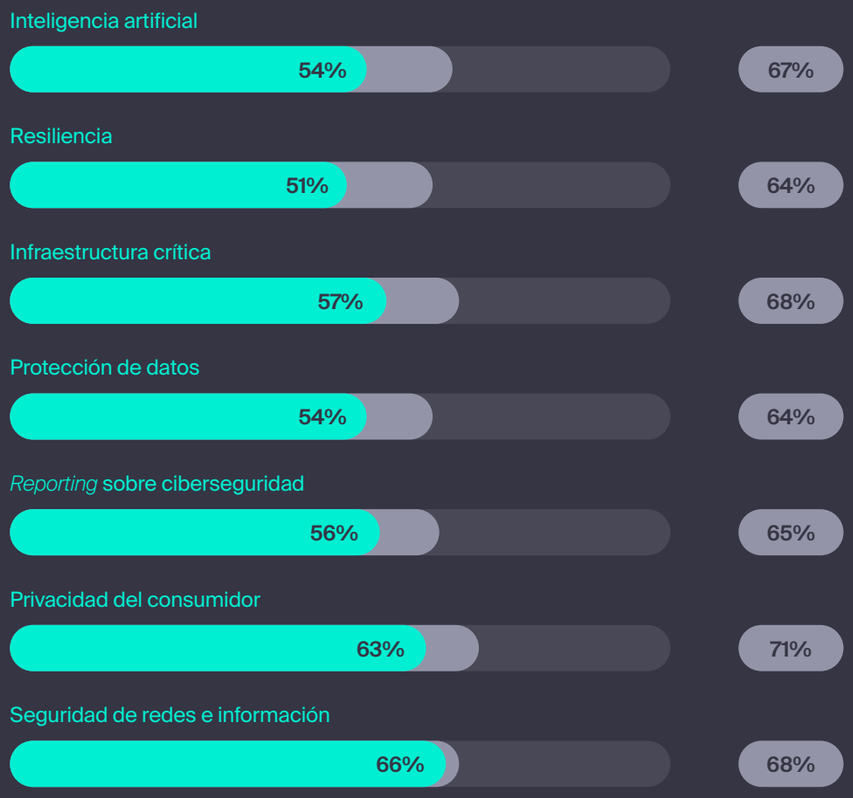
En ese sentido, la regulación está empujando a las organizaciones en la dirección correcta: elevar la disciplina, reducir el riesgo sistémico y aumentar la confianza. Los datos confirman que **una amplia mayoría de organizaciones reconoce que la regulación contribuye de forma efectiva a reducir el riesgo cibernético**. Sin embargo, este mismo impulso ha puesto de manifiesto una tensión estructural que conecta directamente con el mensaje central del informe.

El cumplimiento está avanzando más rápido que la capacidad real de ejecución. La proliferación normativa, su fragmentación entre jurisdicciones y la creciente complejidad de los requisitos están superando la capacidad de muchas organizaciones para absorberlos y traducirlos en control efectivo del riesgo.

Casi siete de cada diez organizaciones reconocen dificultades para implementar las regulaciones existentes, no por falta de conciencia o inversión, sino por la complejidad operativa que introducen: volumen de requisitos, dependencia de terceros, verificación en la cadena de suministro y falta de capacidades internas. A esto se suma una brecha de percepción dentro de las propias organizaciones, donde los equipos de seguridad son sistemáticamente menos optimistas que el resto de la dirección respecto al nivel real de cumplimiento, especialmente en ámbitos críticos como inteligencia artificial, resiliencia e infraestructuras críticas.

Confianza en el cumplimiento normativo de la organización

(% de CEO que tienen alta confianza versus CISO/CSO)



Fuentes: Ercom | Cisco | World Economic Forum | Pwc

Este desajuste es sintomático de un problema más profundo

Los modelos tradicionales de ciberseguridad no fueron diseñados para operar bajo presión regulatoria continua, riesgo interdependiente y entornos altamente dinámicos. El *compliance* evalúa la existencia de controles; el adversario explota su ineficacia operativa. Cuando la seguridad se gestiona como un ejercicio de cumplimiento, la organización puede cumplir y, aun así, seguir estando expuesta.

De esta manera, la regulación deja de ser un mecanismo de reducción de riesgo y se convierte en un amplificador de complejidad. No porque esté mal diseñada, sino porque expone las limitaciones de un modelo que ya no escala. **La dificultad no es cumplir más normas, sino hacerlo con un modelo de seguridad que permita absorber esa exigencia sin fragmentarse**.

69%

de los encuestados considera que **las regulaciones son demasiado complejas o numerosas**, o que resulta difícil verificar si los proveedores externos cumplen con ellas

Fuentes: Ercom | Cisco | World Economic Forum | Pwc

La exposición a riesgos cibernéticos y las exigencias regulatorias están superando la preparación operativa de las organizaciones

Aunque una proporción significativa de empresas identifica la falta de capacidades como una de las principales barreras para la resiliencia, solo una minoría confía en disponer hoy del talento necesario para cumplir sus objetivos de ciberseguridad. Esta brecha convierte **la dependencia de intervención humana en un cuello de botella crítico justo cuando el entorno exige operar a mayor velocidad y escala**.

El efecto combinado es una divergencia cada vez más visible entre exposición, exigencia y preparación. **Incluso organizaciones con altos niveles de inversión y una madurez percibida elevada enfrentan dificultades crecientes para defenderse de forma efectiva**, especialmente en sectores regulados y en regiones donde la presión normativa y la complejidad operativa se intensifican.

La regulación, como se observaba, actúa como amplificador de una debilidad estructural preexistente, haciendo evidente que el modelo tradicional de ciberseguridad no escala cuando la exposición crece, **las obligaciones aumentan y la capacidad humana permanece limitada**.

Este desajuste pone de manifiesto que **la brecha entre exposición real y preparación no puede cerrarse únicamente con más personas, más controles o más cumplimiento**. En un entorno donde el riesgo es continuo, interdependiente y acelerado por la IA, la capacidad de operar y defender sistemas no puede seguir dependiendo de un modelo intensivo en recursos humanos.

La presión regulatoria y el crecimiento de la exposición no hacen sino confirmar que **es necesario un cambio de modelo, capaz de absorber complejidad sin trasladarla íntegramente a la operación**.

Preparación por industria

Maduras

- 6% **Servicios *tech***
- 6% **Medios y comunicación**
- 6% **Recursos naturales**

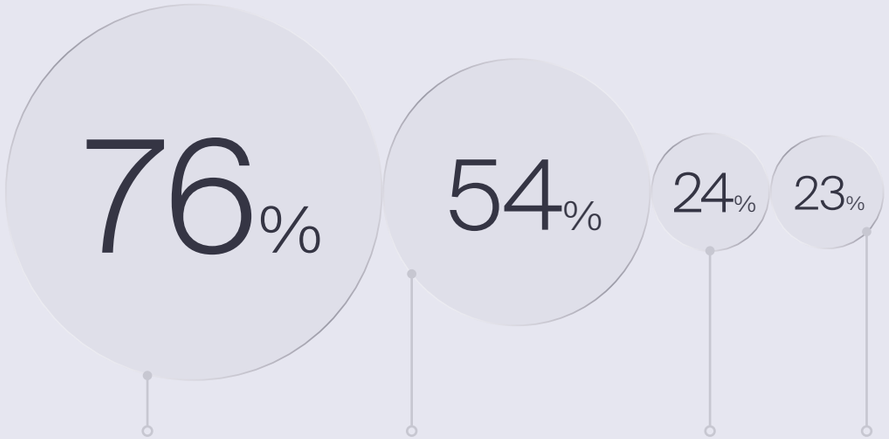
Beginners

- 15% **Comercio mayorista**
- 14% ***Healthcare***

Fuentes: Cisco | World Economic Forum

Más talento no equivale a más resiliencia:
la brecha entre esfuerzo humano y preparación sistémica

Cómo están reaccionando las organizaciones



***Upskilling* interno**
Capacitan y reciclan a sus empleados actuales

Contratación
Contratan profesionales de ciberseguridad con experiencia

Autoformación
Esperan desarrollo de competencias autónomas

Apprenticeships
Promueven programas de aprendizaje o formación dual

Perfiles no tradicionales
Reclutan perfiles fuera de las titulaciones tradicionales

Dónde se traduce realmente en preparación

Mientras las organizaciones intensifican el *upskilling* y la contratación para compensar la escasez de capacidades, **la confianza en la resiliencia frente a incidentes críticos sigue siendo marcadamente desigual** entre países y regiones.

Las economías con mayor madurez institucional y capacidad sistémica absorben mejor ese esfuerzo, las menos preparadas quedan atrapadas en un modelo intensivo en personas que no escala.

Fuentes: Cisco | World Economic Forum

La IA abre una nueva etapa para anticipar amenazas y ampliar la capacidad de defensa

La IA lo cambia todo, incluido quién gana en ciberseguridad

La realidad es que el desarrollo acelerado de la inteligencia artificial está redefiniendo múltiples dominios, y la ciberseguridad no es una excepción. Bien implementada, la IA puede reforzar las capacidades defensivas, apoyar a los equipos humanos y mejorar la detección, la respuesta y la gestión del riesgo. Sin embargo, ese no es el principal desafío al que se enfrentan hoy las organizaciones.

El verdadero punto de inflexión es que **la IA introduce riesgos sistémicos** cuando se despliega de forma desordenada, se gobierna de manera insuficiente o se utiliza de forma ofensiva por parte de actores maliciosos.

Y es que se ha convertido, según una amplia mayoría de líderes, en el principal motor de cambio en ciberseguridad en el corto plazo. No porque sustituya a las tecnologías existentes, sino porque **altera simultáneamente tres dimensiones clave del ecosistema de seguridad**, generando una nueva asimetría entre ataque y defensa.

En primer lugar, la **adopción generalizada de sistemas de IA en los entornos empresariales introduce una superficie de ataque ampliada**. Los modelos, datos, agentes autónomos y flujos automatizados pasan a formar parte del núcleo del negocio, creando nuevas dependencias y vulnerabilidades que los controles tradicionales no estaban diseñados para gestionar.

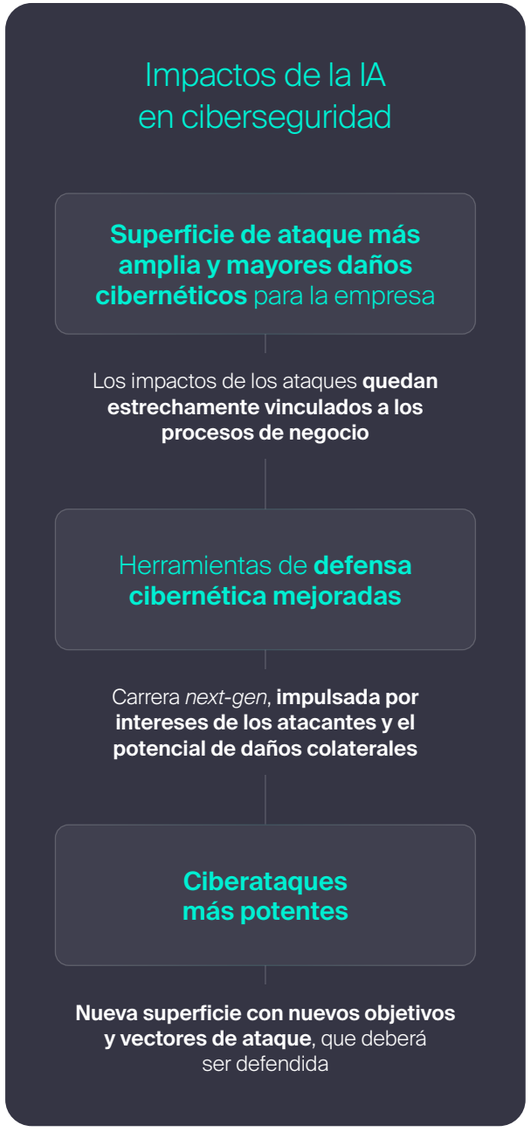
En segundo lugar, **los defensores están empezando a utilizar la IA para fortalecer sus capacidades**. La automatización de tareas analíticas, la mejora de la detección y la aceleración de la respuesta permiten aliviar la presión sobre equipos humanos saturados y operar sobre volúmenes de información inabordables de otro modo.

El mayor impacto, no obstante, se está produciendo en el lado del adversario. Los actores de amenaza están utilizando la IA como **multiplicador de escala, velocidad y sofisticación, automatizando el reconocimiento, la explotación y la ingeniería social dirigida**. El ataque deja de ser secuencial para convertirse en un proceso industrializado, capaz de adaptarse en tiempo real y de operar de forma continua.

La IA **reduce el coste marginal del ataque, incrementa su precisión y elimina muchas de las barreras técnicas** que antes limitaban su alcance.

Estas tres dinámicas ilustran la naturaleza dual de la IA en ciberseguridad. Pero, lejos de equilibrarse, su combinación está **desplazando el conflicto hacia una carrera armamentística impulsada por IA**, en la que la ventaja tiende a concentrarse en quien opera con mayor grado de automatización y menor dependencia de intervención humana.

Sin un gobierno sólido y una integración disciplinada, **la IA no reduce el riesgo, lo redistribuye y, en muchos casos, lo amplifica**. Reconocer esta realidad es imprescindible para entender por qué las organizaciones parten hoy de una posición de desalineación frente a la nueva ciberrealidad.



La carrera de la adaptación: las organizaciones se están quedando atrás

Esta aceleración desalineada no es teórica: se refleja en cómo la IA se gobierna, se opera y se escala en cada lado. Mientras los adversarios la integran como motor central sin fricción, con automatización plena y a velocidad de máquina, muchas organizaciones la adoptan de forma fragmentada y dependiente de ciclos humanos. El resultado es un **conjunto de asimetrías estructurales en el uso de la IA** que colocan a la defensa en desventaja.

Las siguientes cuatro asimetrías explican **por qué hoy la aceleración que introduce la IA favorece al adversario**:

Asimetrías en el uso de la IA

	Defensores	Adversarios	Consecuencia
Gobernanza de la IA	Las organizaciones adoptan IA de forma **distribuida, parcialmente gobernada y con controles inconsistentes** entre negocio, IT y seguridad	Los adversarios utilizan IA **sin restricciones, con experimentación continua y sin fricción operativa** en todo el ciclo de ataque	La **superficie de exposición crece** más rápido que la capacidad real de control y supervisión
Modelo de uso de la IA	La IA se emplea para **apoyar el análisis, manteniendo al humano como punto central** de decisión y validación	**La IA automatiza de extremo a extremo** el reconocimiento, la explotación y la adaptación del ataque	**Los ciclos humanos quedan fuera de ventana** frente a ataques automatizados y persistentes
Velocidad de adaptación	La detección, la decisión y la respuesta **dependen de procesos secuenciales y validaciones manuales**	El adversario **aprende y ajusta su comportamiento en tiempo real** durante el propio ataque	**La defensa reacciona tarde** mientras el ataque evoluciona de forma continua
Escalabilidad operativa	La operación defensiva **escala con personas escasas, formación constante y capacidad operativa limitada**	La operación ofensiva escala **automáticamente, de forma persistente y sin fatiga** humana	El ataque incrementa volumen y presión hasta **saturar la capacidad defensiva**

El siguiente salto en ciberseguridad es convertir la inversión en capacidad real de protección

La exposición crece más rápido que la capacidad de las organizaciones para mantener el control

Las organizaciones operan hoy en un entorno donde la **superficie de ataque se expande** de forma estructural, mientras que la capacidad de control no evoluciona al mismo ritmo.

Las empresas identifican con claridad cuáles son las amenazas que más les preocupan, sin embargo, el problema no es la falta de conciencia, sino una realidad más incómoda: **las amenazas que generan mayor preocupación son, de forma consistente, aquellas para las que las organizaciones se sienten menos preparadas**.

Este desajuste evidencia un problema de fondo, **la preparación no está alineada con la naturaleza del riesgo**. Mientras la exposición se distribuye y se interconecta, el control sigue fragmentado por funciones, tecnologías y responsabilidades. El resultado es una sensación de vulnerabilidad persistente, incluso en organizaciones que han invertido de forma significativa en seguridad.

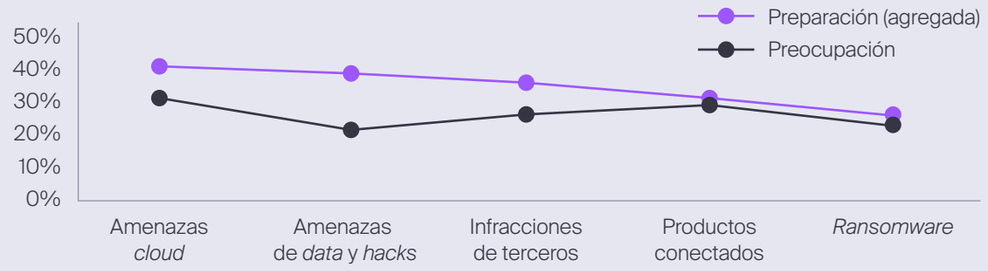
A esta brecha se suma una **desalineación interna en la percepción de prioridades**. Los responsables de seguridad suelen identificar amenazas como el *ransomware* entre los riesgos más críticos dentro de la organización, mientras que esta visión no siempre es compartida por el resto del comité de dirección.

Esta falta de alineación transversal **dificulta la construcción de prioridades comunes y refuerza la necesidad de un lenguaje compartido** entre seguridad y negocio.

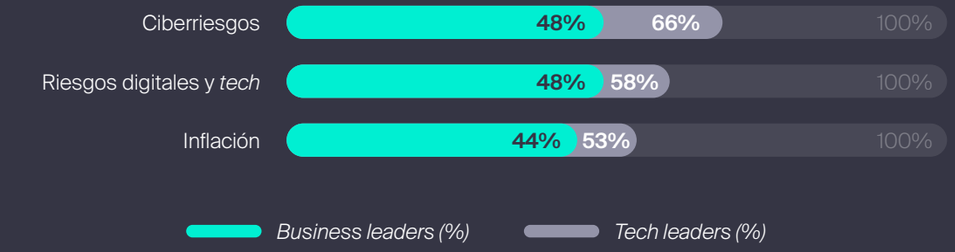
Existe, además, un **consenso amplio sobre la importancia de medir el ciberriesgo** para priorizar inversiones y asignar recursos. Sin embargo, ese consenso rara vez se traduce en práctica efectiva. Solo una minoría de organizaciones cuantifica el riesgo de forma significativa, y cuando lo hace, suele apoyarse en evaluaciones parciales centradas en controles individuales, que ofrecen una visión limitada del riesgo residual.

Las barreras que lo impiden vienen determinadas por la **calidad y disponibilidad del dato, incertidumbre sobre el alcance, preocupaciones legales y, especialmente, falta de confianza en la fiabilidad de los resultados**. A ello se suma la distancia entre lo que la alta dirección necesita para decidir y lo que la función de seguridad es capaz de proporcionar en términos de impacto económico y operativo.

La brecha real entre exposición y control



Prioridades de mitigación del riesgo



Fuentes: Pwc | II | Cisco | Huntress | Crowdstrike

La consecuencia es un punto de partida frágil

A pesar de la creciente preocupación, la mayoría de las organizaciones reconoce dificultades para implantar de forma consistente prácticas básicas de ciberresiliencia y, sin una resiliencia transversal, el negocio permanece expuesto a amenazas capaces de comprometer la operación en su conjunto.

Las organizaciones no parten desde la falta de conciencia, sino desde una **incapacidad estructural para transformar esa conciencia en control efectivo**, en un entorno de riesgo continuo, interdependiente y amplificado por la IA.

La cuantificación del ciberriesgo como facilitador

El 88% de los ejecutivos reconoce que permite **priorizar inversiones** y comunicar el riesgo en términos alineados con la tolerancia del negocio, mientras que el 87% la considera clave para asignar recursos allí donde el impacto potencial es mayor.

Cuantificar el riesgo **transforma la ciberseguridad en una capacidad estratégica demostrable y comparable**, anclando decisiones en criterios económicos consistentes y no en percepciones fragmentadas.

Fuentes: Pwc | II | Cisco | Huntress | Crowdstrike

Sorprendentemente, una mayor inversión no se está traduciendo en preparación operativa

Partiendo de una exposición creciente y de una conciencia cada vez mayor del riesgo, cabría esperar que el aumento sostenido de la inversión en ciberseguridad se tradujera en una mejora equivalente de la capacidad real de protección. Sin embargo, en la práctica, esto no está ocurriendo. **Las organizaciones invierten más que nunca en tecnología, servicios y cumplimiento, pero siguen mostrando dificultades para operar con eficacia en un entorno de ataque continuo**.

La razón no es la falta de recursos, sino la **desconexión entre inversión y modelo operativo**. La inversión refuerza componentes del sistema (herramientas, controles o procesos), pero no siempre construye capacidades reales para detectar, responder y mantener la continuidad del negocio bajo presión. Esta brecha se manifiesta de forma recurrente en cuatro dimensiones clave.

Aunque el 77% de las organizaciones incrementó su presupuesto en ciberseguridad en 2025, la mayor parte del crecimiento se concentra en **aumentos tácticos del 10% o menos**. Este patrón revela una inversión defensiva, diseñada para sostener el *statu quo*, no para transformar la capacidad operativa.

30% ha incrementado un 6-10% su presupuesto

8% ha incrementado más de un 15% su presupuesto

Fuentes: Pwc | II | Cisco | Huntress | Crowdstrike

Dimensiones de la ruptura

1

Readiness percibida frente a *readiness* operativa

Las organizaciones confunden preparación con controles, auditorías y marcos. Sin embargo, esta percepción no se traduce en una mejora real de la detección, respuesta o resiliencia.

La preparación efectiva se mide en capacidad de operar bajo ataque, no en cumplimiento ni en volumen de controles

2

Cumplimiento normativo frente a capacidad real de ejecución

La regulación ha impulsado inversiones y elevado el nivel mínimo de seguridad, pero cumplir no equivale a estar preparado. El *compliance* evalúa la existencia de controles, no su eficacia frente a ataques reales.

Esto genera una falsa sensación de seguridad sin mejorar la capacidad operativa

3

La cuantificación del ciberriesgo como promesa incumplida

Pocas organizaciones logran traducir sus mediciones en impacto económico accionable. La cuantificación se apoya en métricas parciales que no guían prioridades ni decisiones de negocio.

Sin una medición creíble, la preocupación por el riesgo no se convierte en acción sostenida

4

Brecha de capacidades: el límite del modelo humano-dependiente

La inversión sigue centrada en personas y procesos manuales, un modelo que no escala frente a ataques automatizados por IA. La defensa depende de ciclos humanos mientras el ataque opera a velocidad de máquina.

Sin automatización y orquestación, la inversión incrementa complejidad, no resiliencia

La desalineación entre exposición real y capacidad efectiva de control no es el resultado de decisiones puntuales ni de carencias aisladas. Es la consecuencia directa de operar con un modelo de ciberseguridad diseñado para un entorno que ya no existe. **Intentar cerrar esta brecha incrementando inversión, añadiendo controles o reforzando el cumplimiento solo optimiza un enfoque estructuralmente insuficiente**.

Fuentes: Pwc | II | Cisco | Huntress | Crowdstrike

Una organización más segura se construye desde la forma de pensar, decidir y operar

Más allá de la seguridad reactiva: cuatro capacidades fundamentales

La transformación que exige la ciberseguridad actual no es, ante todo, tecnológica. **Las organizaciones no están fallando por carecer de soluciones, sino por seguir operando desde una mentalidad concebida para un entorno ya obsoleto**. Los tiempos en los que la ciberseguridad se consideraba como algo perimetral y orientado a desplegar controles, gestionar excepciones y responder a incidencias como eventos puntuales ya no existen para las corporaciones.

En este contexto, reforzar controles o incrementar inversión sin cambiar la forma de entender el riesgo y la operación solo optimiza un modelo que ya no escala. La ciberseguridad deja de ser una función técnica y **se convierte en una capacidad operativa del conjunto de la organización, que afecta a arquitectura, gobierno, operación y continuidad del negocio**.

Por eso, **el cambio no puede ser parcial ni limitado a un área concreta, debe ser global e integral**, porque el riesgo es transversal y se materializa allí donde confluyen personas, procesos, tecnología y terceros. Adoptar nuevas herramientas sin transformar la mentalidad corporativa genera una falsa sensación de avance y refuerza la fragilidad del modelo.

Para lograr este cambio de mentalidad, **se necesitan nuevas vías concretas para materializar este cambio.** Aplicarlas de forma coherente permite pasar de una lógica de protección reactiva a una de operación resiliente bajo ataque continuo.

No adoptarlas implica aceptar, de forma implícita, una pérdida progresiva de control frente a una realidad que ya no espera:

Vías de transformación

1. **Confianza cero e identidad continua**
   En un entorno distribuido la identidad es el nuevo perímetro, y **confiar una sola vez equivale a perder el control durante todo el ciclo de acceso**

2. **Automatización defensiva y operación a velocidad de máquina**
   Los ciclos humanos ya no son compatibles con ataques automatizados, y **sin automatización la defensa queda estructuralmente fuera de ventana**

3. **Resiliencia por diseño y capacidad de operar bajo interrupción**
   El ataque no es una excepción, sino una condición permanente, **y el control se mide por la capacidad de absorber impacto y continuar operando**

4. **Criptografía y protección preparadas para un entorno poscuántico**
   La confidencialidad y **la integridad a largo plazo no pueden depender de supuestos criptográficos que ya están en proceso de ruptura**

Zero Trust e identidad continua: la base del nuevo modelo de control

La primera transformación imprescindible en la ciberseguridad reinventada es abandonar definitivamente la confianza implícita. El modelo tradicional se construyó sobre la premisa de que era posible definir un perímetro y que, una vez dentro, usuarios y sistemas podían considerarse confiables. Este podía funcionar en entornos cerrados y relativamente estables, pero **se rompe de forma irreversible en ecosistemas *cloud*, híbridos y remotos, donde las identidades interactúan de manera constante y distribuida**.

La mayoría de las brechas actualmente se producen por el abuso de credenciales legítimas. De hecho, **en 2025 se han robado 1.800 millones de credenciales de 5,8 millones de dispositivos**, consolidando el abuso de identidades legítimas como vector dominante. Todo esto ocurre en un entorno acelerado por la inteligencia artificial, donde la suplantación, el phishing avanzado y la automatización reducen drásticamente las barreras de entrada.

La confianza cero introduce un cambio radical, donde **se asume que la brecha es posible además de probable y que, por tanto, cada acceso debe verificarse de forma continua, contextual y dinámica**. La identidad deja de validarse en el momento del *login* y pasa a evaluarse en tiempo real, incorporando señales como comportamiento, ubicación, estado del dispositivo o nivel de riesgo.

Este enfoque permite **ajustar permisos de manera adaptativa, limitar el impacto de credenciales comprometidas y reducir de forma significativa la toma de cuentas**, incluso cuando el atacante ya ha superado los primeros controles.

89%

de las brechas en 2025 **se originan por robo de credenciales**

Fuentes: Capgemini | Orange | Segurilatam | Ciber Safety | Avatier | Vectra

Esta vía se materializa en arquitecturas *identity-first*

Humanos, máquinas y servicios se gobiernan bajo principios de verificación continua y mínimo privilegio. Este enfoque no busca únicamente reforzar el acceso, sino recuperar el control en entornos donde el perímetro ha desaparecido.

En ecosistemas SaaS, *cloud* y BYOD, la identidad es el único punto de control persistente y todo lo demás es transitorio. **Sin una evaluación dinámica del acceso basada en contexto y riesgo, la organización pierde visibilidad y capacidad de contención** en el mismo momento en que un atacante obtiene credenciales válidas.

La criticidad de este cambio es inmediata. En un panorama donde la mayoría de los ataques ya no intentan entrar, sino operar como usuarios legítimos, seguir tratando la identidad como un control puntual deja a la organización estructuralmente expuesta.

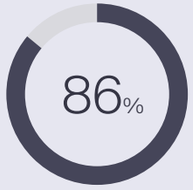
La combinación de credenciales robadas, privilegios excesivos y accesos persistentes convierte cualquier compromiso inicial en un **problema sistémico, difícil de detectar y aún más difícil de contener**.

No adoptar esta mentalidad permite al atacante aprovechar la confianza heredada del modelo anterior sin necesidad de explotar vulnerabilidades técnicas complejas. Una vez dentro, el movimiento lateral, la exfiltración y la escalada de impacto se producen sin fricción y, en muchos casos, sin generar alertas significativas.

La confianza cero con identidad continua no es, por tanto, una mejora incremental ni una recomendación avanzada. **Es el punto mínimo a partir del cual la ciberseguridad vuelve a ser operable en la nueva realidad**. Sin ella, cualquier otro pilar se apoya en una base inestable, y el control se pierde no de forma abrupta, sino silenciosa y progresiva.

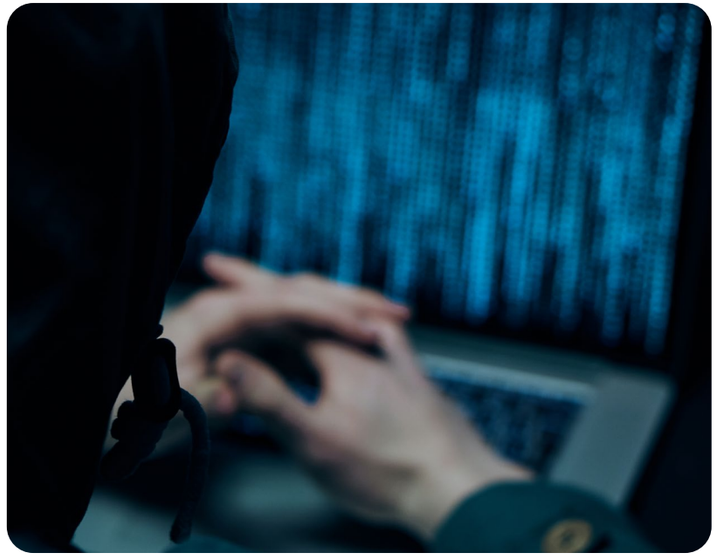
Qué impacto está teniendo esta práctica de transformación

menos incidentes de toma de cuentas en organizaciones que aplican autenticación continua frente a modelos tradicionales



de los usuarios **reportan una experiencia de autenticación más positiva** tras implementar verificación continua de identidad

hasta un 40% de reducción en *tickets* de soporte relacionados con accesos, disminución significativa del tiempo dedicado a revisiones y bloqueos



Fuentes: Capgemini | Orange | Segurilatam | Ciber Safety | Avatier | Vectra

1 Confianza cero e identidad continua

Para que la confianza cero sea operable, debe traducirse en una arquitectura capaz de evaluar, decidir y aplicar políticas de acceso de forma dinámica y distribuida. En lugar de concentrar la seguridad en un perímetro estático, **el control se desplaza a cada interacción entre usuarios, sistemas y recursos, independientemente de dónde se encuentren**. Esto exige separar claramente la toma de decisiones de acceso, la definición de políticas y su aplicación en tiempo real, apoyándose en múltiples señales de contexto, riesgo y comportamiento.

Es con la **arquitectura *Zero Trust* con la que se materializa esta vía**, un modelo donde ningún acceso se asume como confiable, todas las peticiones se evalúan de forma continua y el control se ejerce allí donde ocurre la interacción, no donde termina la red.

Automatización defensiva y operaciones a velocidad de máquina, control sin latencia humana

Definir correctamente **quién accede a qué no es suficiente** si la organización no puede ejercer ese control a la velocidad necesaria. El modelo tradicional de ciberseguridad asumía que los ciclos humanos —detección, análisis, decisión y respuesta— eran compatibles con la dinámica del ataque, pero ese supuesto se ha roto de forma definitiva.

Hoy, los adversarios operan de manera automatizada, apoyados por IA, completando ciclos de ataque en minutos mientras **la detección humana sigue produciéndose, de media, días después**. Ahora, el tiempo se convierte en otro vector de riesgo.

La nueva mentalidad exige aceptar que las personas no pueden seguir siendo el centro de la ejecución defensiva. Su papel debe dejar de ser reaccionar alerta a alerta y pasar a diseñar, entrenar y supervisar sistemas capaces de detectar y responder de forma autónoma. Visto de esta manera, **la automatización defensiva no es una optimización operativa ni una mejora incremental del Centro de Operaciones de Seguridad (SOC), es la única forma de igualar la carrera frente a adversarios** que ya operan a velocidad de máquina.

Esta vía es plasmada con modelos de seguridad distribuida y automatizada, donde la detección, la correlación y la respuesta se orquestan en tiempo real a través de plataformas capaces de procesar millones de eventos diarios sin intervención humana.

La automatización permite aislar *endpoints*, bloquear accesos, contener movimientos laterales o iniciar procesos de recuperación en segundos, reduciendo de forma drástica el impacto del incidente y minimizando el error humano, responsable de la mayoría de las brechas. Al mismo tiempo, **libera a los equipos de seguridad de la fatiga operativa, permitiéndoles centrarse en análisis estratégico y mejora continua**.

La necesidad de seguridad distribuida refuerza este cambio de mentalidad. En entornos híbridos, *multi-cloud*, con IoT, OT y trabajo remoto, el control debe aplicarse allí donde ocurre la interacción.

Agentes distribuidos, arquitecturas SASE y *enforcement* en el *edge* permiten aplicar políticas contextuales en cada acceso, **limitando la propagación del ataque incluso cuando el adversario ya ha obtenido credenciales legítimas**.

Sin automatización y operación a velocidad de máquina, la organización queda permanentemente obsoleta, ya que detectará y responderá tarde y actuará cuando el impacto sea incontrolable.

En un entorno donde la IA reduce barreras de entrada, acelera el *phishing*, facilita la suplantación y automatiza la explotación, **seguir operando con defensas manuales equivale a aceptar una pérdida estructural de control**.

La automatización defensiva de la seguridad es una condición básica para que la ciberseguridad vuelva a ser operable en la nueva realidad.

95%

El error humano sigue siendo responsable de hasta el **95% de las brechas.**

Impacto de la IA y la automatización en la reducción de pérdidas

La adopción efectiva de IA y automatización defensiva **reduce tiempos de respuesta hasta en 80 días y disminuye de forma material el impacto económico de las brechas (1,9 millones de dólares).**

Promedio global 4.44 **M de $**

Organizaciones que **utilizan IA y automatización** de forma extensiva 3.62 **M de $**

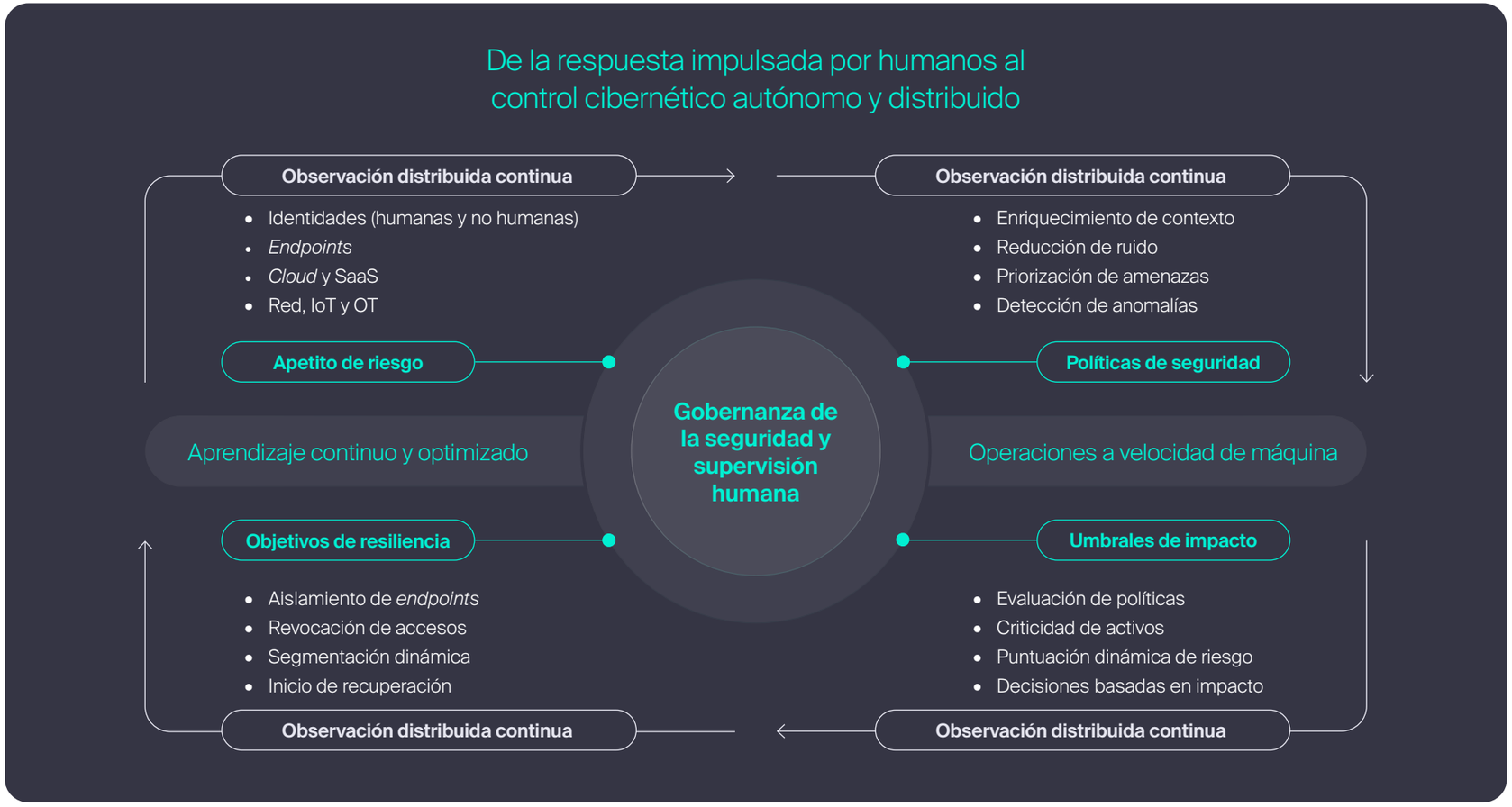
Organizaciones **sin IA** ni automatización de seguridad 5.52 **M de $**

Coste medio por brecha

Fuentes: Fortinet | Capgemini | Orange | IBM | II

2 Automatización defensiva a velocidad de máquina

Las personas definen políticas, umbrales de riesgo y objetivos de contención y las plataformas automatizadas ejecutan detección, correlación y respuesta de forma continua y autónoma. **El control deja de ser reactivo y pasa a ser permanente, distribuido y orquestado, capaz de actuar en segundos allí donde se produce la amenaza**.



Resiliencia por diseño y capacidad de operar ante interrupciones

Incluso con identidad continua y automatización defensiva, asumir que los incidentes pueden evitarse siempre es una ilusión. El modelo actual resulta frágil en un entorno donde la mayoría de los ataques ya no se producen por fallos técnicos evidentes, sino por el abuso de credenciales legítimas y accesos internos difíciles de distinguir del comportamiento normal. **En una realidad acelerada por la IA y el *cloud*, la brecha deja de ser una anomalía y pasa a ser un escenario plausible y recurrente**.

La resiliencia introduce un cambio de mentalidad donde **se debe aceptar el compromiso como punto de partida y diseñar la organización para seguir operando cuando el ataque ocurre, no solo para intentar evitarlo**. Esto implica asumir fallos parciales, limitar el impacto desde el origen y priorizar los servicios críticos frente a una lógica de protección homogénea. Se busca integrar la resiliencia desde el diseño de la arquitectura, los procesos y la toma de decisiones.

La resiliencia operativa en ciberseguridad se hace tangible en **arquitecturas pensadas para absorber el impacto y recuperarse de forma controlada**: microsegmentación que evita la propagación lateral, copias de seguridad inmutables que impiden la extorsión, mecanismos de *failover* automático y orquestación de la recuperación que reducen los tiempos de inactividad de días a horas.

La seguridad deja de verse como una capa añadida y se convierte en un atributo intrínseco del sistema. En este modelo, **la capacidad de recuperación es tan importante como la capacidad de detección, y ambas se diseñan para operar bajo presión**.

La relevancia de esta vía no es únicamente técnica o estratégica. Es, cada vez más, regulatoria y estructural. **Marcos como DORA y NIS2 reflejan un cambio profundo en cómo se entiende la ciberseguridad desde el regulador**: ya no basta con demostrar que existen controles preventivos, políticas o certificaciones, ahora las organizaciones deben probar que pueden seguir operando bajo condiciones de disrupción real. La resiliencia deja de evaluarse sobre el papel y pasa a medirse en la práctica.

Estas normativas introducen una exigencia explícita de resiliencia operativa *end-to-end*, que abarca anticipación, absorción del impacto, recuperación y adaptación continua. No se trata solo de tener planes de continuidad documentados, sino de someter a la organización a pruebas periódicas, simulaciones de escenarios adversos y validación de capacidades reales de recuperación.

Operar sin resiliencia *by design* puede pasar a ser un incumplimiento potencial, con implicaciones directas en sanciones, supervisión reforzada y responsabilidad de la alta dirección.

La estabilidad financiera, la continuidad del servicio y la protección del cliente se convierten en objetivos explícitos de la ciberseguridad, alineando de forma directa riesgo tecnológico y riesgo de negocio.

En organizaciones no resilientes, **cada incidente se transforma en una crisis sistémica donde las interrupciones prolongadas, escalado descontrolado del impacto, pérdidas económicas significativas y exposición regulatoria creciente**. La falta de capacidad para demostrar recuperación efectiva erosiona la confianza de clientes, socios y supervisores, amplificando el daño más allá del incidente inicial.

Por el contrario, **las organizaciones que diseñan para operar bajo interrupción no solo limitan el impacto técnico, sino que convierten la resiliencia en una ventaja competitiva**. Recuperan antes, mantienen el servicio cuando otros colapsan y refuerzan su credibilidad frente a reguladores y mercado. En la nueva ciberrealidad, la diferencia ya no está entre sufrir o no incidentes, sino entre ser capaz de absorberlos y continuar operando o ver comprometida la viabilidad del negocio.

Resiliencia incentivada mediante sanción

50%

de los ataques de *ransomware* **en 2025 se dirigieron a sectores críticos y esenciales**

Esenciales

Multas de hasta **10 millones de euros o el 2% del volumen de negocio** anual global

Importantes

Multas de hasta **7 millones de euros o el 1,4% del volumen de negocio** anual global

Fuentes: World Economic Forum | National Cyber Security Center | Google | AO Data Cloud | AENOR

3 Ciberresiliencia por diseño

La resiliencia debe materializarse tanto en la operación (cómo se anticipa, absorbe, recupera y aprende la organización) como en las capas que la hacen posible: liderazgo, gobierno, priorización del riesgo y coordinación del ecosistema. Este enfoque exige **abandonar visiones parciales y traducir el concepto de resiliencia en un sistema coherente, donde la capacidad de operar a gran velocidad se sostiene sobre decisiones organizativas, marcos de gobierno y fundamentos de seguridad alineados con el negocio**.

Criptografía poscuántica y protección a largo plazo: un control que debe resistir el paso del tiempo

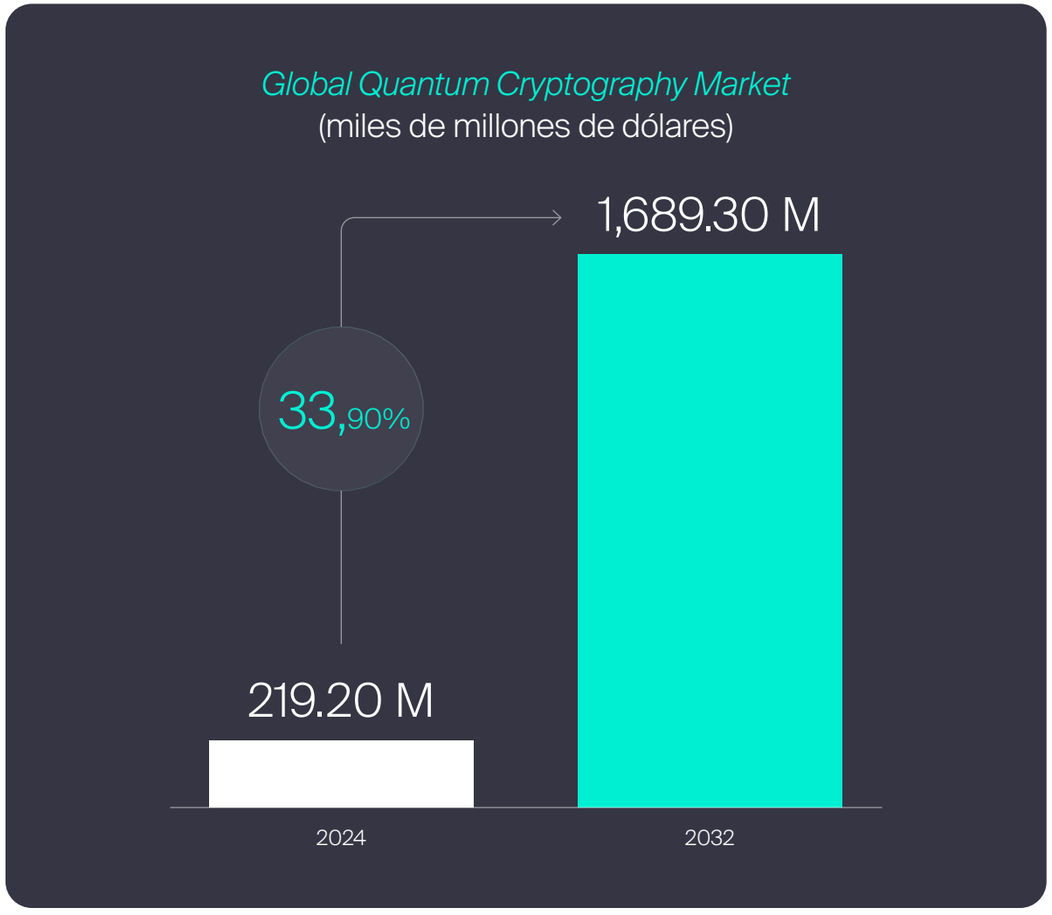
El cuarto y último pilar introduce una dimensión que el modelo tradicional de ciberseguridad ha tendido a ignorar: la durabilidad de la confianza en el tiempo. Durante décadas, la criptografía ha sido el cimiento invisible sobre el que se construyen identidades, comunicaciones, transacciones y protección de datos. El modelo heredado asumía que estos cimientos eran estables y que proteger el presente era suficiente.

La amenaza no reside en un fallo gradual de los algoritmos actuales, sino en su obsolescencia abrupta. Algoritmos ampliamente utilizados como RSA o ECC, hoy considerados seguros, **pueden ser quebrados de forma eficiente mediante algoritmos cuánticos**. La proyección de ordenadores cuánticos con capacidades suficientes en el horizonte futuro convierte esta amenaza en una cuestión de cuándo, no de si. En ese escenario, claves que hoy requerirían milenios de computación clásica para romperse podrán descifrarse en horas o incluso minutos.

Este cambio corrige uno de los supuestos más profundos del modelo anterior: que el cifrado protege la información durante todo su ciclo de vida. En realidad, muchos activos críticos (como datos sanitarios, contratos financieros, propiedad intelectual, certificados raíz) tienen una vida útil de tan solo décadas.

La estrategia conocida como ***harvest now, decrypt later*** (recolectar ahora, descifrar después) permite a adversarios avanzados recolectar hoy grandes volúmenes de información cifrada con el objetivo de descifrarla cuando la capacidad cuántica lo permita. Cuando eso ocurra, la pérdida de confianza será retroactiva e irreversible.

La criptografía poscuántica introduce una nueva fuerza, la de anticipar la ruptura antes de que sea real. No se trata de una migración puntual ni de un reemplazo inmediato de todos los algoritmos, sino de construir cripto-agilidad como capacidad estructural. Esto implica conocer dónde y cómo se usa la criptografía, evaluar la exposición de los activos a largo plazo y diseñar transiciones progresivas hacia algoritmos resistentes a la computación cuántica, manteniendo compatibilidad operativa.



Fuentes: McKinsey | II | DMR | Fortinet | II | Data Bridge Market

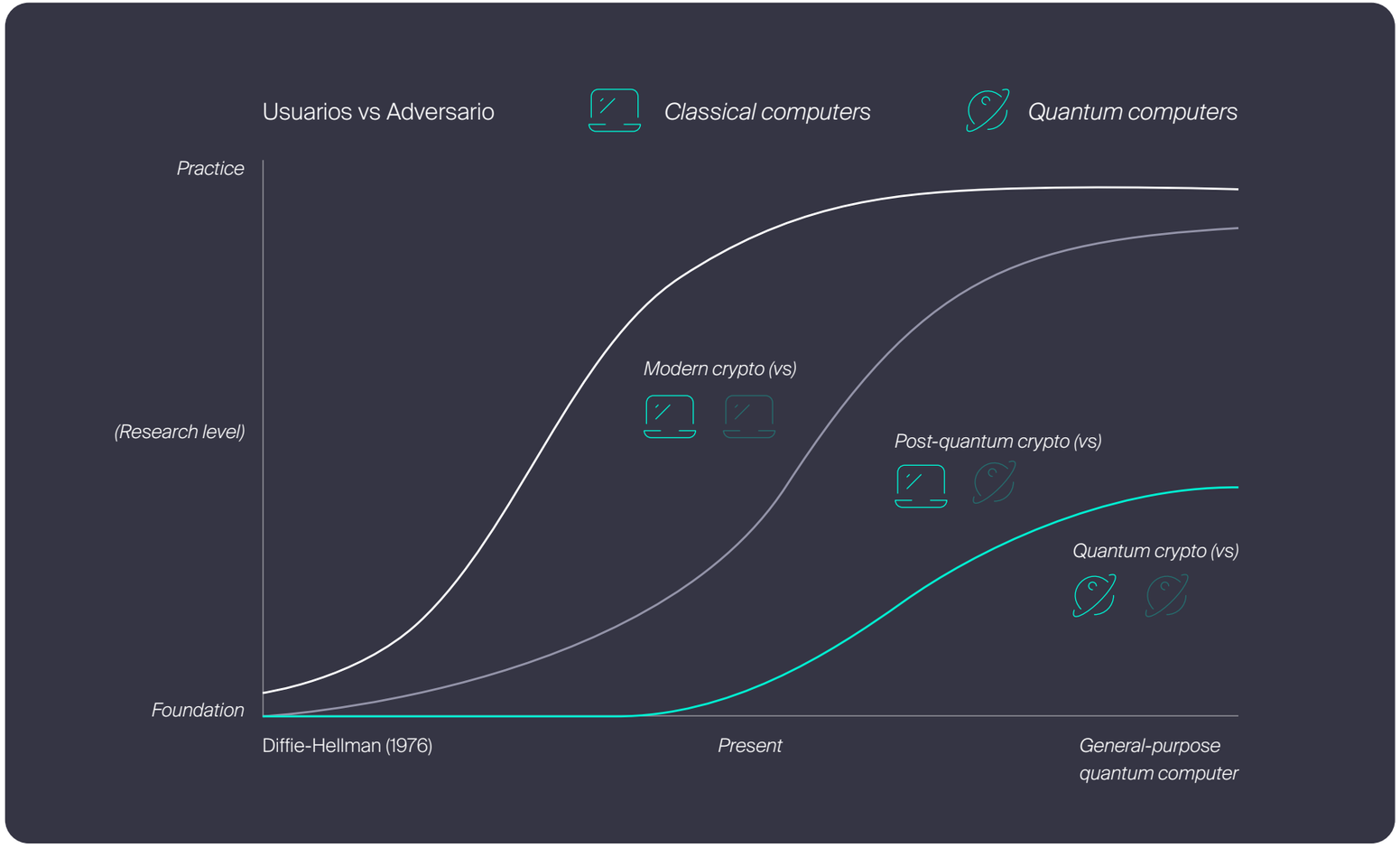
Las tendencias que sustentan esta vía ya son tangibles

El **NIST finalizó en 2024 los estándares de criptografía poscuántica** (Kyber, Dilithium, Falcon, SPHINCS+), marcando el inicio formal de la transición.

Certificados digitales emitidos hoy, con ciclos de vida de cinco a diez años, quedarán expuestos si no se planifica su migración desde ahora. Paralelamente, **grandes proveedores tecnológicos ya están desplegando esquemas híbridos** (clásico + PQC) en protocolos como TLS 1.3, anticipando un escenario donde la agilidad criptográfica será un requisito de interoperabilidad, no una opción.

Tanto en EE.UU. como en Europa, **los marcos regulatorios empiezan a exigir explícitamente capacidades de cripto-agilidad como parte de la resiliencia digital**. La desafección progresiva de algoritmos clásicos, la obligación de auditar inventarios criptográficos y la protección de infraestructuras críticas convierten la preparación poscuántica en una responsabilidad ejecutiva.

No adoptar esta vía tiene un riesgo singular, y es que no se manifiesta como un incidente inmediato, sino como una pérdida diferida y sistémica de confianza. **Cuando los supuestos criptográficos caen, no se compromete solo la seguridad futura, sino la existente**. Datos históricos, contratos vigentes y evidencias regulatorias pueden quedar expuestos de forma simultánea.



Fuentes: McKinsey | II | DMR | Fortinet | II | Data Bridge Market

4 Protección poscuántica

En la implicación práctica de esta estrategia no basta con que la información esté cifrada hoy: debe seguir estándolo mañana. **El problema real reside en su capacidad para resistir un cambio tecnológico que ya está en marcha**. Cuando la vida útil del dato supera la del algoritmo que lo protege, la seguridad deja de ser binaria y pasa a ser temporal.

De la seguridad tradicional a la protección a largo plazo

Criptografía tradicional

La criptografía tradicional **protege la información en el presente**, asumiendo que los algoritmos actuales seguirán siendo seguros en el tiempo.

Sin embargo, a medida que se alarga la vida útil de los datos, **este enfoque expone a las organizaciones a un riesgo diferido**.

PQC

La PQC desplaza el foco **hacia la confidencialidad a largo plazo**, incorporando algoritmos resistentes a la computación cuántica y modelos híbridos.

Esto permite anticiparse a la disrupción criptográfica y proteger el valor de la información más allá del horizonte tecnológico actual.

Ejecución empresarial

Su adopción efectiva requiere **visibilidad, priorización y gobierno**.

Las organizaciones deben identificar **dónde reside la criptografía, priorizar la protección de datos** con mayor valor y longevidad, **e integrar capacidades híbridas de forma progresiva** en diversas áreas.

Anticipación al futuro

Cuando se integra desde el diseño, **la seguridad se convierte en una capacidad duradera**.

La organización preserva la confidencialidad a lo largo de los ciclos tecnológicos, **se alinea con la regulación** futura y garantiza que la confianza digital sobreviva a la disrupción cuántica.

Solo una seguridad diseñada para sobrevivir a los cambios tecnológicos, capaz de adaptarse, evolucionar y anticipar la disrupción, **puede preservar de forma sostenida la confianza de clientes, reguladores y ecosistemas digitales**

El futuro de la ciberseguridad se demuestra en la capacidad del negocio para seguir avanzando

De la visión a la ejecución: cómo operarán las organizaciones

Los cuatro pilares definen las condiciones mínimas para que la ciberseguridad vuelva a ser operable en una realidad de ataque continuo, aceleración tecnológica y presión regulatoria creciente. Juntos, corrigen los límites estructurales del modelo anterior y establecen un nuevo marco mental: **el control se basa en identidad continua, automatización, resiliencia operativa y protección a largo plazo**.

Sin embargo, reconocer la necesidad de este nuevo modelo no equivale a haberlo adoptado. El principal reto para la mayoría de las organizaciones es ejecutivo. **La brecha entre entender qué debe cambiar y ser capaz de implementarlo de forma coherente sigue siendo amplia**. Iniciativas aisladas, adopciones parciales o enfoques puramente tecnológicos no solo retrasan la transformación, sino que refuerzan la falsa sensación de avance que ha caracterizado al modelo anterior.

La pregunta ya no es qué pilares son necesarios, sino **cómo se traducen en capacidades reales, cómo se integran en la operación diaria y cómo se priorizan en función del riesgo, la madurez y el contexto de cada organización**.

Cómo construir el nuevo modelo sin romper la operación

Recuperar el control básico

- Identidad continua y *Zero Trust* operativo
- Eliminación de confianza implícita
- Control mínimo de accesos, privilegios y exposición

Diseñar para la interrupción

- Capacidad real de continuidad
- Segmentación, recuperación, pruebas
- Alineación con DORA / NIS2

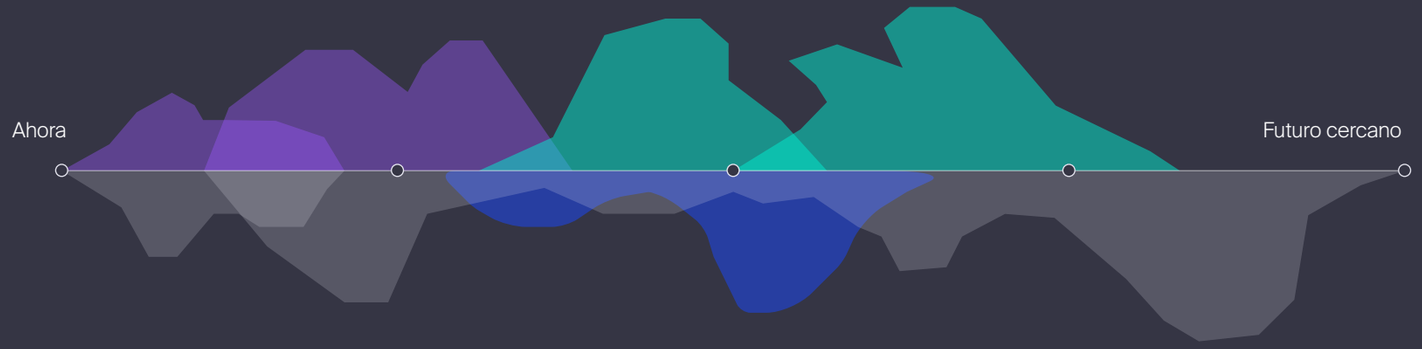
Cerrar la brecha temporal

- Automatización defensiva
- Seguridad distribuida
- Reducción de tiempos de detección y contención

Proteger el futuro

- Criptoagilidad
- Preparación poscuántica
- Protección de datos de larga vida

En un entorno de riesgo continuo, el *roadmap* de ciberseguridad debe priorizar aquellas capacidades que aumentan de forma tangible el control efectivo, reducen la asimetría frente al adversario y evitan riesgos irreversibles, y gobernarse como un modelo operativo transversal con métricas orientadas a impacto, tiempo y continuidad del negocio, **asumiendo que la ciberseguridad reinventada es un sistema vivo y no un estado final**.



Softtek®

softtek.com