

Ciberseguridad para una operación más compleja, autónoma y distribuida

Digital Trust Insights 2027, edición México

Ciberseguridad para una operación más compleja, autónoma y distribuida

46%

identifica la falta de claridad sobre responsabilidades compartidas con proveedores.

47%

permitiría a agentes de IA ejecutar de manera independiente acciones de ciberdefensa de bajo riesgo.

Los resultados de la encuesta ***Digital Trust Insights 2027, edición México,*** muestran que la ciberseguridad está ampliando su alcance más allá de la protección de sistemas y datos.

La creciente dependencia de proveedores críticos, la incorporación de agentes de inteligencia artificial (IA) y el desafío de sostener operaciones cada vez más distribuidas están llevando a las organizaciones a replantear cómo gestionan el riesgo y la resiliencia.

Por ejemplo, aunque la proporción de líderes encuestados en México que prevé aumentar su presupuesto de ciberseguridad disminuyó de 86% en 2026 a 74% en 2027, el 58% señala la protección frente a ataques habilitados por la IA entre los factores que influirán en sus prioridades de gasto durante los próximos 12 meses. Además, el 46% anticipa cambios en el seguro cibernético, la respuesta a incidentes y la planeación del manejo de crisis.

43%

cuenta con planes de continuidad operativa formalizados e integrados frente al panorama actual de ciberamenazas.

54%

señala al ciberriesgo como un tema permanente en la agenda del consejo de administración.

Los datos de la encuesta apuntan a que **la resiliencia depende cada vez más de comprender qué activos, sistemas, proveedores y agentes forman parte de la operación, cómo se conectan y quién responde por ellos.** A partir de esta visibilidad, el reto consistiría en coordinar personas, procesos y tecnologías bajo escenarios de riesgo más complejos.

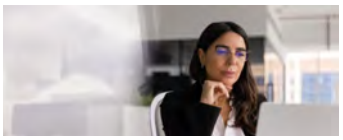
Al mismo tiempo, persisten áreas de oportunidad para integrar el riesgo en las decisiones que impactan la operación y el negocio. En México, menos de la mitad reporta haber implementado a escala organizacional capacidades para integrar información de riesgo cibernético en la gestión de riesgos empresariales (ERM, por sus siglas en inglés) y en la toma de decisiones (48%), así como para vincular esos riesgos con servicios, procesos o activos críticos (47%).



Contenido



01 Más allá del perímetro:
fortalecer la resiliencia ante dependencias externas 05



02 Autonomía de la IA:
la redefinición del control 09



03 La prueba real
de la continuidad es la ejecución 15



04 El ciberriesgo
está presente; el reto es traducirlo al negocio 19



05 Agenda estratégica:
cuatro capacidades para una ciberseguridad más resiliente 21

Acerca de este reporte 23

Contáctanos 23

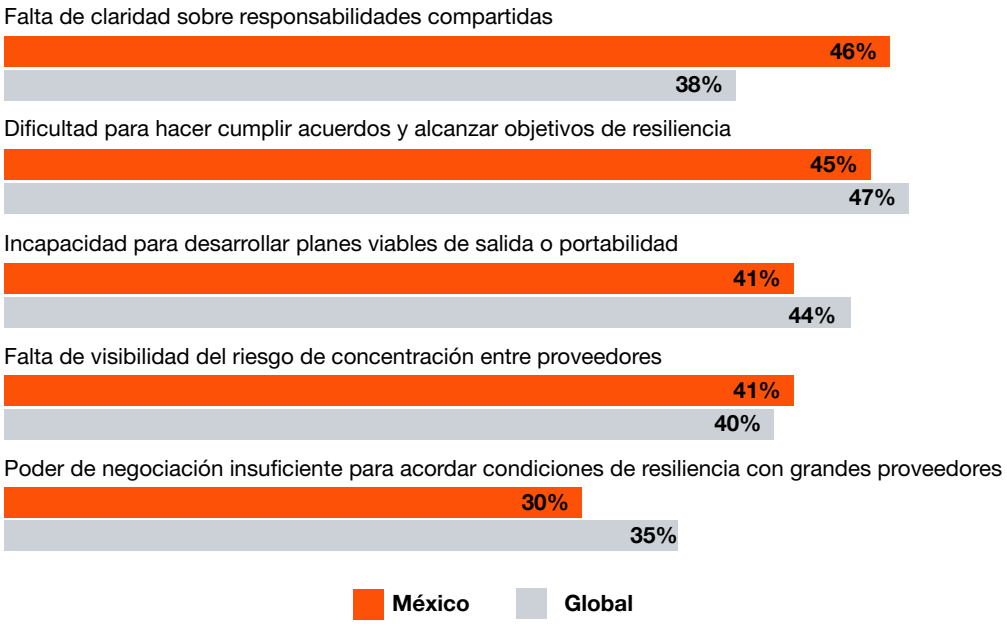


01

Más allá del perímetro: fortalecer la resiliencia ante dependencias externas

Las organizaciones recurren cada vez más a terceros para ejecutar procesos, almacenar información y sostener servicios esenciales. Si bien esta expansión del ecosistema digital tiende a ayudar al negocio, también puede incrementar la exposición a riesgos que difícilmente pueden mitigarse solo con controles internos.

¿Qué dificulta mantener la resiliencia con proveedores críticos?



Fuente: *PwC 2027 Global Digital Trust Insights*, base: 97 (México); 2,725 (global). Se muestran las cinco respuestas con mayor porcentaje de selección a la pregunta: “Al gestionar proveedores de servicios externos críticos, ¿cuáles son los mayores desafíos de tu organización para mantener la resiliencia operativa?”.

Los resultados sugieren que el desafío ya no se centra únicamente en identificar a los proveedores estratégicos. También implica dimensionar el impacto de una interrupción de sus servicios, evaluar las capacidades de recuperación y contar con alternativas para mantener la continuidad operativa.

Conforme más funciones esenciales se distribuyen entre plataformas y recursos externos, es relevante identificar aquellos puntos cuya interrupción podría impactar múltiples procesos o áreas de la organización. Esta evolución también se observa en decisiones de carácter estratégico.

Gestionar terceros ya no es solo una decisión operativa

Los cambios en el entorno global están llevando a las organizaciones a revisar la forma en que gestionan sus relaciones con terceros. En el caso de los ejecutivos encuestados en México, el 51% incluye cambios en la gestión de proveedores y la cadena de suministro dentro de las áreas de su estrategia que prevén modificar en los próximos 12 meses frente al contexto geopolítico.

Las tres principales acciones que los participantes implementarían en el mismo periodo para gestionar el riesgo cibernético en la cadena de suministro son:

1. Fortalecimiento de la ciberseguridad en los procesos de desarrollo y entrega de *software*: 50%

2. Implementación de monitoreo continuo del riesgo cibernético de proveedores: 41%

3. Endurecimiento de los requisitos contractuales de ciberseguridad: 41%

Aunado a las medidas previstas, **fortalecer la resiliencia operativa suele requerir un conocimiento más preciso de los componentes externos que soportan las funciones, operaciones e información clave,** así como de las capacidades disponibles para recuperar la operación cuando alguno de ellos deja de estar disponible.

Este entendimiento permite definir responsabilidades con mayor claridad, establecer mecanismos de coordinación y mejorar la toma de decisiones cuando una afectación interrumpe las funciones clave del negocio.

En el panorama actual de la ciberseguridad, fortalecer la seguridad de la operación también abarca la definición de límites de actuación, criterios de escalamiento y controles de supervisión aplicables a sistemas de inteligencia artificial cada vez más autónomos.





02 Autonomía de la IA: la redefinición del control

La creciente capacidad de la inteligencia artificial para ayudar a ejecutar tareas y tomar decisiones plantea nuevos desafíos para la gestión de riesgos.

En un entorno de creciente escrutinio sobre los alcances y riesgos asociados a esta tecnología, cobran relevancia temas que trascienden su adopción, como validar sus resultados, delimitar los niveles de autonomía que se le delegan y establecer responsabilidades sobre las decisiones que puede llegar a ejecutar.

El reto de entender cómo opera la IA en la práctica

Las políticas y marcos de control son un punto de partida para gobernar la IA, pero no necesariamente ofrecen evidencia suficiente ni aseguramiento sobre la forma en que estos sistemas operan en condiciones reales. Con una mayor evolución de los casos de uso, resulta cada vez más importante para las empresas verificar que:

- Los resultados generados se mantienen dentro de los parámetros previstos.
- Los controles responden de manera proporcional a los riesgos asociados a cada implementación.

Los hallazgos de la *Digital Trust Insights 2027* indican que estos temas ya forman parte de las agendas de ciberseguridad de los líderes de tecnología en México, aunque no de forma generalizada.

El gobierno y el cumplimiento de la IA responsable ocupan el primer lugar (50%), seguido por la detección y gestión de sistemas o herramientas de IA utilizados fuera de los procedimientos formales de supervisión (*shadow AI*) (44%). También destacan el fortalecimiento de plataformas y la protección e integridad de los datos de entrenamiento (40%, respectivamente).

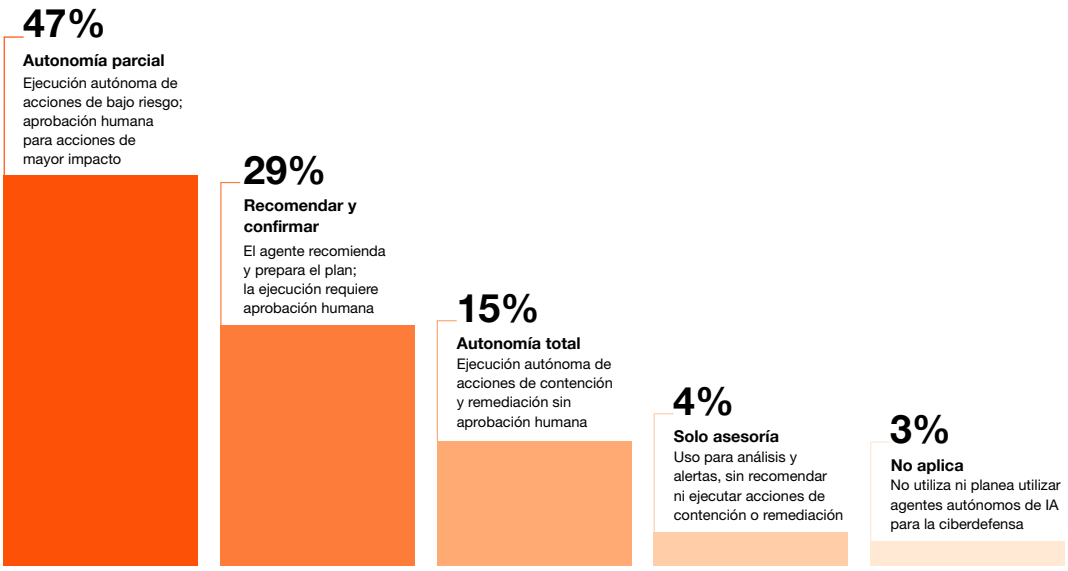
Estas prioridades revelan que el uso responsable de la inteligencia artificial requiere una supervisión, gobierno y control cada vez más maduros. Una base como esta permite a las organizaciones evaluar qué decisiones y acciones pueden asumir sistemas con mayor independencia.

¿Hasta dónde dejar actuar a la IA?

Las organizaciones en México avanzan hacia formas más sofisticadas de incorporar la inteligencia artificial en sus operaciones. Con ello, l**a ciberdefensa representa uno de los primeros ámbitos de aplicación práctica, dado que puede requerir equilibrar la velocidad de respuesta frente a amenazas y la supervisión sobre acciones potencialmente críticas.**

La distribución de respuestas señala que la autorización de agentes de IA para actuar en ciberdefensa no suele plantearse como una decisión binaria entre autonomía total e intervención humana permanente, sino como un espectro con distintos grados de participación humana.

Niveles de autonomía autorizados en ciberdefensa



Fuente: *PwC 2027 Global Digital Trust Insights*, base: 142 (México). Se muestra la distribución de respuestas por nivel de confianza a la pregunta: "¿Qué afirmación refleja mejor tu nivel de confianza para autorizar a agentes de IA autónomos la ejecución de acciones de ciberdefensa sin aprobación humana?". Los porcentajes pueden no sumar 100% debido al redondeo.

Entre las funciones donde los líderes de tecnología anticipan permitir una mayor actuación autónoma de agentes de IA durante los próximos 12 meses destacan:

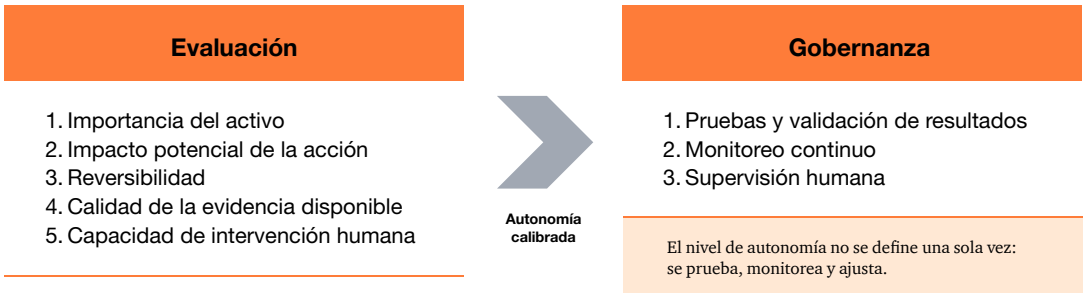
- Remediación de *malware* y sistemas: 59%
- Aplicación de parches y cambios de configuración: 50%
- Enriquecimiento y correlación de inteligencia de amenazas: 47%
- Cuarentena o eliminación de correos de *phishing*: 46%

La concentración en estas funciones apunta hacia una disposición a autorizar actividades asociadas con la respuesta ante amenazas, manteniendo mayores reservas frente a acciones con implicaciones más amplias para la operación.

Esta disposición convive con desafíos importantes para extender estos niveles de autonomía en operaciones de seguridad. **Las principales barreras identificadas por los ejecutivos en México son la confiabilidad y madurez de la tecnología (61%), la posibilidad de manipulación adversaria de los sistemas de IA (49%) y los desafíos relacionados con la responsabilidad y atribución en la toma de decisiones (44%).**

El alcance de la autonomía difícilmente puede definirse mediante un criterio único. En la práctica, suele requerir una evaluación del nivel de riesgo asociado a cada caso de uso.

Factores para calibrar la autonomía



Fuente: análisis PwC.

La IA puede actuar, la responsabilidad sigue siendo humana

La implementación de este tipo de sistemas también introduce nuevas preguntas sobre quién responde por sus resultados, bajo qué criterios operan y cómo se supervisan sus acciones.

En México, las áreas de tecnología y los equipos especializados en IA aparecen con mayor frecuencia como responsables del gobierno y riesgo de la IA, con el 31% en ambos casos.

Fuente:
PwC 2027 Global Digital Trust Insights, base: 88 (México).

Gestión de identidades no humanas

Cuando un sistema puede consultar información, interactuar con herramientas externas, modificar configuraciones o activar respuestas, requiere una identidad verificable y permisos acordes con su función. Esto implicaría mantener inventarios actualizados, delimitar accesos y verificar que los privilegios otorgados sean consistentes con las tareas que puede ejecutar.

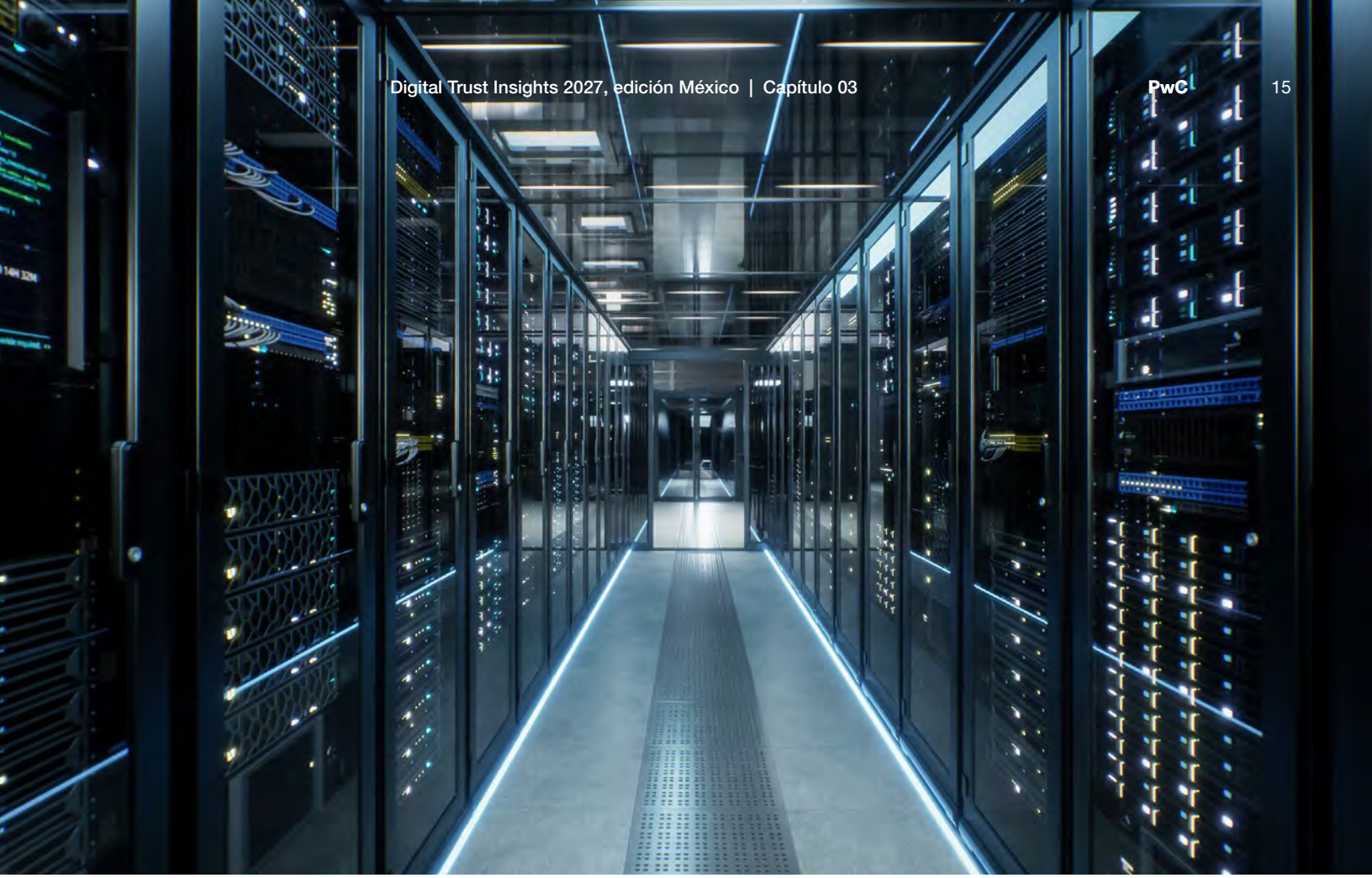
Según el reporte *Annual Threat Dynamics 2026: Cyber threats in motion*, los actores de amenazas recurrirán cada vez más a la inteligencia artificial para atacar identidades no humanas, incluidas las cuentas de servicio, integraciones automatizadas e identidades utilizadas por agentes de IA.

La definición de responsabilidades y mecanismos de supervisión no depende únicamente de la tecnología; también está relacionada con las competencias humanas para gobernar estos sistemas, interpretarlos y trabajar con ellos de manera efectiva.

En este sentido, el 62% de los encuestados en México señala que la inversión en herramientas habilitadas por la IA y la capacitación para trabajar en ellas son una prioridad para el desarrollo y la retención del talento en ciberseguridad, mientras que el 51% indica el fortalecimiento de la cultura de ciberseguridad.

La presencia de la inteligencia artificial y de sistemas más autónomos ayuda a redefinir parte de los retos en ciberseguridad relacionados con su gobierno, supervisión y responsabilidad. Al mismo tiempo, refuerza la importancia de mantener la continuidad y la resiliencia ante eventos disruptivos.



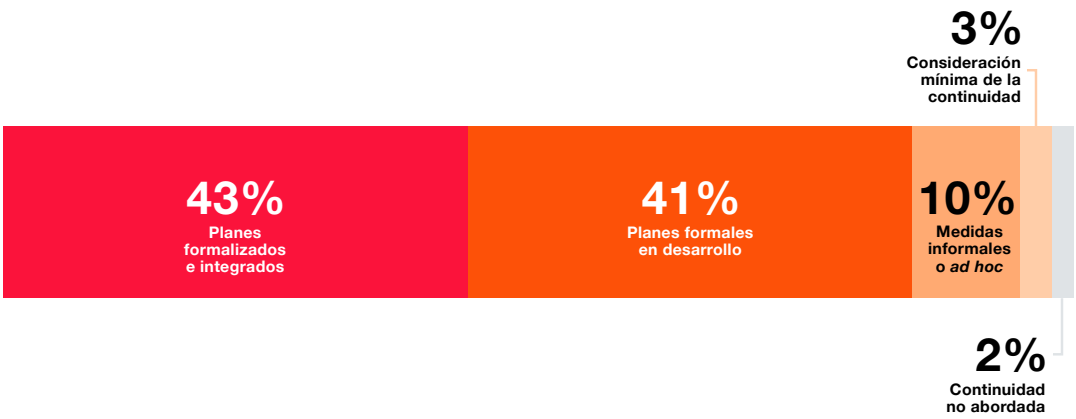


03 La prueba real de la continuidad es la ejecución

Comprender qué sostiene la operación es solo uno de los desafíos ante las actuales ciberamenazas. La siguiente pregunta suele ser qué tan preparada está una organización para responder, coordinarse y recuperarse cuando alguno de esos componentes deja de estar disponible.

De acuerdo con los resultados de la *Digital Trust Insights 2027, edición México*, una parte importante del liderazgo afirma haber avanzado hacia esquemas de continuidad incorporados a la organización, mientras que una proporción similar reporta que estas iniciativas se encuentran en proceso de consolidación.

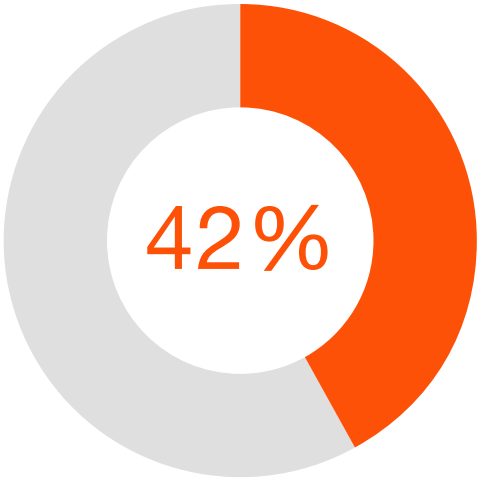
¿Cuál es el estado de los planes de continuidad frente a ciberamenazas?



Fuente: *PwC 2027 Global Digital Trust Insights*, base: 97 (México). Se muestra el porcentaje de organizaciones según su nivel de avance en la planificación de continuidad operativa, con base en la pregunta: "¿Cuál de las siguientes opciones describe mejor el enfoque de tu organización respecto a la planificación de la continuidad operativa en respuesta al panorama actual de ciberamenazas?".

La diferencia entre contar con procedimientos documentados y estar preparado para ejecutarlos puede hacerse más visible a través de ejercicios capaces de revelar brechas operativas, problemas de coordinación o supuestos que no siempre son evidentes en la documentación.

La preparación suele depender menos de la existencia de un plan y más de la eficacia para ejecutarlo en condiciones reales. Factores como el entrenamiento de los equipos, las pruebas realizadas y la participación de actores clave de negocio, tecnología y seguridad pueden influir de manera significativa en este sentido.



Realiza periódicamente ejercicios realistas de respuesta ante incidentes para evaluar su nivel de preparación.

Fuente: *PwC 2027 Global Digital Trust Insights*, base: 142 (México). Se muestra el porcentaje de quienes seleccionaron "totalmente de acuerdo" a la pregunta: "¿En qué medida estás de acuerdo o en desacuerdo con las siguientes afirmaciones?".

No obstante, la respuesta ante una interrupción tampoco se limita al ámbito interno. En cuanto a los cambios que el liderazgo encuestado prevé implementar, durante los próximos 12 meses, para gestionar el riesgo cibernético de la cadena de suministro, el 23% incluye la incorporación de proveedores en ejercicios de respuesta a incidentes y gestión de crisis.

Esta práctica puede contribuir a validar protocolos de coordinación y comunicación que son particularmente relevantes cuando eventos que afectan la continuidad involucran capacidades fuera del control directo de la organización.

La resiliencia se está diseñando desde la arquitectura

La preparación para responder a una disrupción no solo se construye mediante planes, ejercicios o esquemas de coordinación. En México, algunas de las acciones previstas en el corto plazo se relacionan con decisiones de arquitectura tecnológica. Estas apuntan a diversificar dependencias, ampliar las opciones de recuperación y sostener operaciones clave.

Entre las principales se encuentran:

1.

Adopción de estrategias multinube o de nube híbrida para evitar la dependencia de un único proveedor o jurisdicción: 56%

2.

Implementación de capacidades de redundancia y respaldo de datos y tecnología a nivel local o regional: 47%

3.

Restricción del acceso a datos y tecnología según la ubicación geográfica o el usuario: 44%

4.

Migración a proveedores de nube soberanos o regionales: 40%

La preparación, la recuperación y las decisiones de arquitectura pueden aumentar las alternativas disponibles frente a incidentes. Sin embargo, para que puedan contribuir a la resiliencia organizacional, es fundamental integrarlas en los procesos de gestión y toma de decisiones.

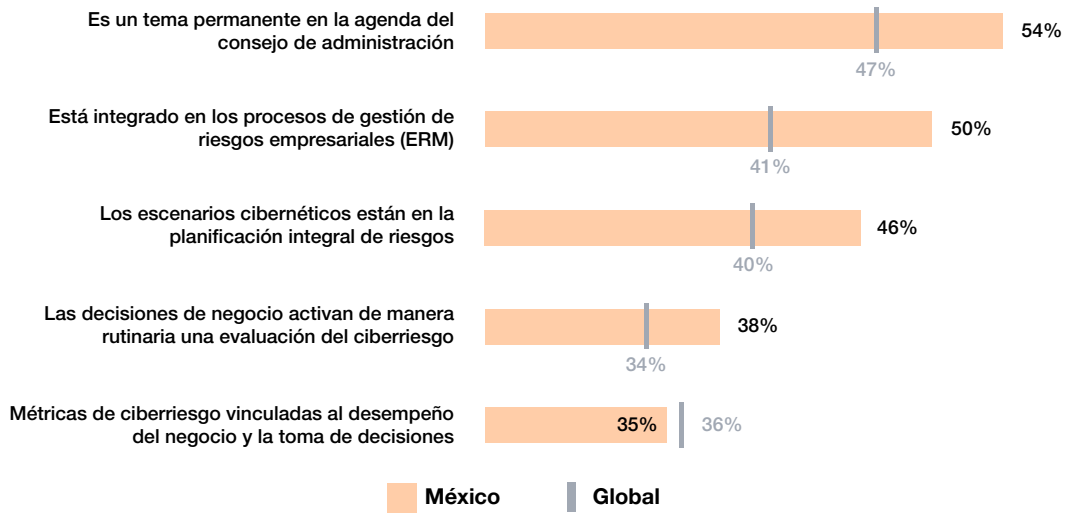




04 El ciberriesgo está presente; el reto es traducirlo al negocio

Un hallazgo relevante a nivel global y local es que, aunque el ciberriesgo ocupa un lugar estable en los espacios de dirección de la mitad de los encuestados, su integración pierde intensidad en cuanto a los criterios que orientan el desempeño y las decisiones del negocio.

Dónde y cómo se incorpora el ciberriesgo en la organización



Fuente: *PwC 2027 Global Digital Trust Insights*, base: 142 (México); 3,934 (global). Se muestra el porcentaje de cinco respuestas de quienes seleccionaron "totalmente de acuerdo" a la pregunta: "¿Hasta qué punto estás de acuerdo o en desacuerdo con las siguientes afirmaciones?".

Para influir de manera más directa en las decisiones del negocio, el ciberriesgo puede presentarse en términos de impacto operativo, financiero o estratégico, y no únicamente desde una perspectiva técnica.

Menos de la mitad de los líderes en México afirman que sus organizaciones cuentan con procesos para interpretar el ciberriesgo, integrarlo en la gestión empresarial y vincularlo con elementos concretos del negocio. Entre esas acciones se encuentran:

- Asignación clara de responsabilidades para interpretar y actuar sobre señales de riesgo: 49%
- Integración de hallazgos de riesgo cibernético en la gestión de riesgos empresariales y decisiones: 48%
- Mapeo de riesgos en servicios, procesos o activos críticos: 47%
- Traducción de métricas técnicas en el impacto empresarial: 42%

Cuando se traduce en consecuencias concretas para la operación, la inversión o el crecimiento, el ciberriesgo puede incorporarse con mayor facilidad en las decisiones sobre adquisiciones, expansión a nuevos mercados, lanzamiento de productos o exposición financiera.



05 Agenda estratégica: cuatro capacidades para una ciberseguridad más resiliente

A lo largo de los hallazgos del reporte aparece una misma tensión: muchas organizaciones ya han incorporado el ciberriesgo en sus estructuras, estrategias y procesos, pero todavía enfrentan el desafío de traducir esos esfuerzos en prácticas más efectivas para supervisar riesgos, responder a eventos críticos y respaldar la toma de decisiones.

En este contexto, los resultados permiten identificar cuatro áreas de enfoque complementarias que pueden contribuir a una gestión y coordinación de ciberseguridad más sólida:

ANTICIPAR

01 Fortalecimiento de la resiliencia compartida

La dependencia de terceros, plataformas y ecosistemas externos otorga mayor relevancia a la visibilidad sobre concentraciones críticas, la coordinación con proveedores y las alternativas de respuesta y recuperación ante un incidente.

02 Delimitación de la autonomía

Escalar la autonomía de la inteligencia artificial depende de establecer límites, criterios de autorización y mecanismos de supervisión proporcionales al riesgo de cada acción. De forma que permitan anticipar impactos y preservar el control sobre decisiones relevantes.

RESPONDER

03 Preparación para la ejecución

La preparación ante una interrupción se fortalece cuando los planes se complementan con entrenamiento, ejercicios realistas, coordinación entre actores clave y validación sobre condiciones cercanas a la operación.

04 Interpretación del ciberriesgo

Fortalecer esta capacidad suele implicar la traducción de las señales técnicas a un contexto de negocio, vincularlas con impactos potenciales y convertirlas en información útil para anticipar riesgos, asignar responsables y priorizar decisiones.

OPERACIÓN

GOBIERNO Y DECISIÓN



Acerca de este reporte

La edición 2027 de la encuesta *Digital Trust Insights* fue diseñada para conocer la perspectiva sobre los desafíos y oportunidades para fortalecer y transformar la ciberseguridad de las organizaciones durante los próximos 12 meses.

Los resultados se basan en respuestas de 3,934 líderes de negocio y tecnología en 71 territorios, incluyendo 142 participantes en México, recopiladas entre el 6 de mayo y el 15 de julio de 2026.

Los participantes en México representan una variedad de industrias, entre ellas: tecnología (15%), ingeniería y construcción (8%), gestión de activos y patrimonio (8%), bienes de consumo (8%) y manufactura industrial (7%).

Las respuestas en México forman parte de una muestra distribuida en siete regiones. La proporción de participantes es: Europa Occidental (32%), Norteamérica (26%), Asia Pacífico (18%), Latinoamérica (12%), Europa Central y Oriental (4%), África (5%) y Medio Oriente (3%).

La encuesta *Digital Trust Insights*, anteriormente conocida como *Global State of Information Security Survey* (GSISS), cumple 29 años como el estudio más longevo sobre ciberseguridad empresarial. Es también el más grande de la industria y el único que reúne la perspectiva de ejecutivos de negocio junto con líderes de tecnología y seguridad.

Contáctanos

Fernando Román

Socio Líder de Cyber, Data and Tech Risk, PwC México

fernando.roman@pwc.com

LinkedIn