Digital Trust Insights 2022

Estrategia de ciberseguridad en las organizaciones: cómo simplificar los procesos para su implementación.

pwc

www.pwc.com.ar

Índice

Introducción	03
¿Puede el CEO marcar la diferencia en la gestión de la ciberseguridad?	06
¿Es tu compañía demasiado compleja para ser asegurada?	10
¿Tu organización está protegida contra los principales riesgos?	12
¿Conocés los riesgos que presentan para tu organización la relación con los terceros y la cadena de suministro?	18
Nuestros servicios	23
Acerca de la encuesta	25
Contactos	25

Introducción

Los ciberdelincuentes son cada vez más sofisticados: su objetivo es encontrar vulnerabilidades en los sistemas y redes de las empresas para luego explotarlas para su beneficio. Las consecuencias de un ciberataque son mayores a medida que aumenta la complejidad e interdependencia de los sistemas. Sin embargo, muchos de los riesgos con los que nos enfrentamos pueden prevenirse si ponemos en marcha distintas prácticas y controles.

Les presentamos una nueva edición de la encuesta global Digital Trust Insights, que revela dos ejes clave para 2022 en materia de ciberseguridad. Por un lado, las empresas aumentarán su presupuesto cibernético y por otro lado se espera que este año aumenten los ciberataques, por encima de los niveles récord de 2021.

Si consideramos a la ciberseguridad como un todo unificado, veremos que, en realidad, se trata de una preocupación de toda la empresa, de cada área y de cada empleado. Para hacer frente a los desafíos mencionados nos centraremos en cuatro preguntas.

1. ¿Puede el CEO marcar la diferencia en la gestión de la ciberseguridad?
2. ¿Cuán compleja es tu organización para ser asegurada?
3. ¿Tu organización está protegida contra los principales riesgos?
4. ¿Conocés los riesgos derivados de terceros y de la cadena de suministro?

El 69% de las organizaciones en el mundo prevé aumentar sus inversiones en ciberseguridad para 2022 en comparación con el 55% del año 2021. Para la región de Latinoamérica el valor fue del 71%. A nivel global, más de una cuarta parte (26%) estima un aumento del gasto cibernético de un 10% o más, mientras que en Latinoamérica la cifra es mayor (32%). Solo el 12% indicó un gasto igual al del año pasado (a nivel global), en tanto que para Latinoamérica dicha opción representó un 7%.

Las organizaciones saben que los riesgos relacionados al ciberdelito son cada vez mayores. Más del 50% espera un aumento en los ciberincidentes para 2022, por encima de los niveles de 2021. En lo que respecta a Latinoamérica y en Argentina en particular, los números fueron bastante similares, arrojando en promedio 46% y 41% respectivamente.

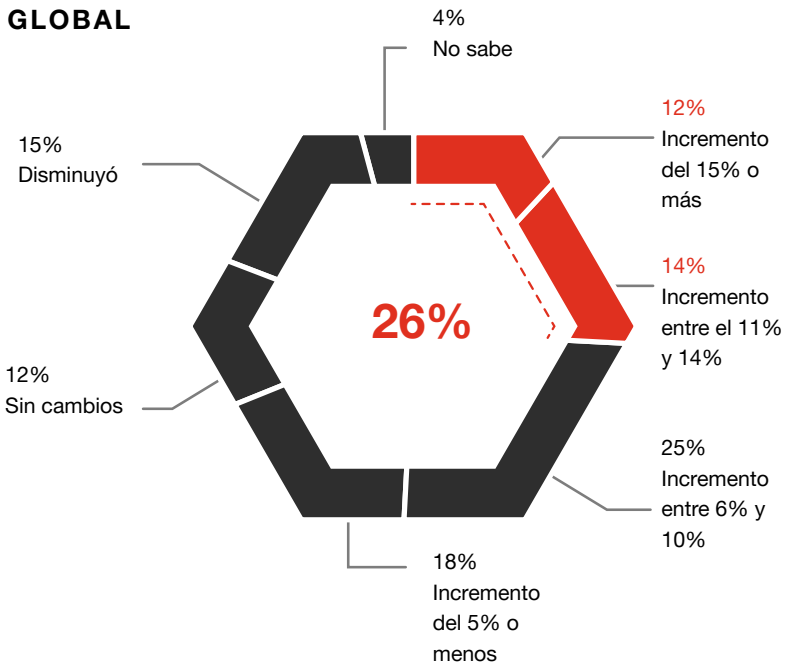
Los atacantes son cada vez más sofisticados, sondean nuestros sistemas y redes buscando vulnerabilidades. Cualquiera sea el motivo, desde un servidor desprotegido hasta una falla en el código que controla el acceso a las carteras criptográficas, los ciberdelincuentes utilizarán todos los medios a su disposición, tanto tradicionales como ultra sofisticados, para explotarlos.

Las consecuencias de un ataque aumentan a medida que las interdependencias de nuestros sistemas se vuelven cada vez más complejas. Las infraestructuras críticas son especialmente vulnerables. Y, sin embargo, muchos de los ciberataques que estamos viendo todavía se pueden prevenir con prácticas de ciberseguridad sólidas y controles estrictos.

GRÁFICO 1

¿Cuáles serán las variaciones de su presupuesto cibernético en 2022?

GLOBAL



LATINOAMÉRICA

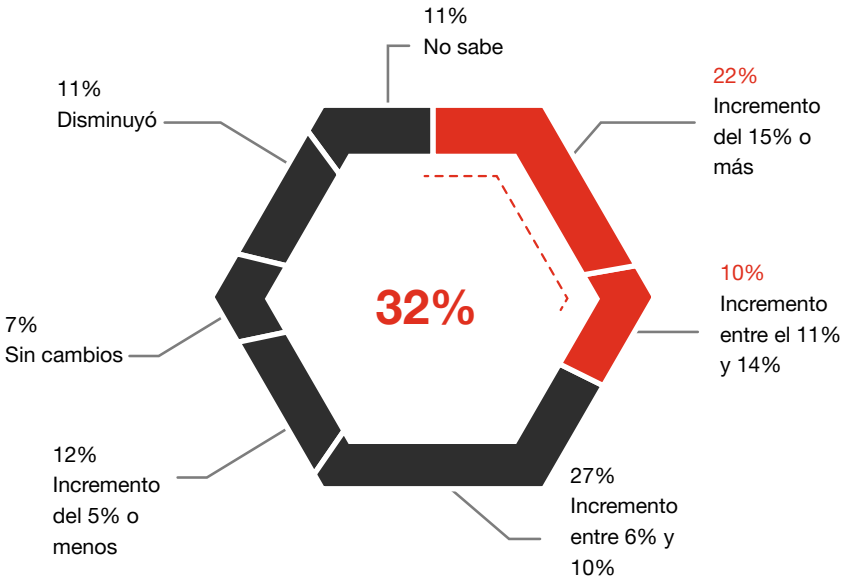
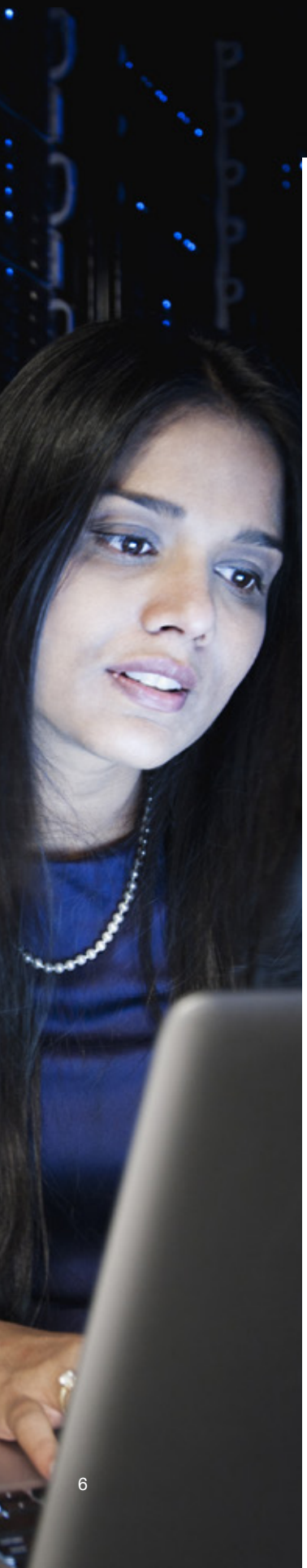


GRÁFICO 2

¿En qué medida su organización está priorizando inversiones en los siguientes temas?



¿Puede el CEO marcar la diferencia en la gestión de la ciberseguridad?

Si bien la mayoría de los CEOs encuestados para la presente edición manifestó como “significativo” su nivel de compromiso para mitigar los riesgos relacionados con la ciberseguridad; no opinan de la misma manera el resto de los ejecutivos, que perciben un involucramiento del CEO y la alta dirección más reactiva que proactiva en esta materia, sobre todo tras un incidente de seguridad con impacto en el negocio o ante requerimientos regulatorios.

No obstante, el informe señala que esta brecha va reduciéndose ya que, según el 46% de los entrevistados en el mundo, las interacciones con el CEO en materia de ciberseguridad han aumentado en los últimos dos años.

¿Cuánto apoyo brinda el CEO al liderazgo del CISO?

Los directores ejecutivos tenían más probabilidades que el resto de los directores y gerentes de calificar como "significativo" su nivel de apoyo en seis áreas. Por ejemplo, a nivel global el 37% de los CEOs afirmó que brindan un apoyo significativo para "garantizar los recursos adecuados, la financiación y la prioridad suficiente" para la ciberseguridad, mientras que solo el 30% de los no CEOs estuvieron de acuerdo en que sus directores ejecutivos lo hicieran. Para Latinoamérica dichos valores estuvieron en torno al 34% para los CEOs y 38% para los no CEOs.

El 34% de los CEOs a nivel global dice que brindan una ayuda significativa al liderazgo de ciberseguridad al "reducir la incertidumbre de los inversores con respecto a los riesgos cibernéticos organizacionales", mientras que sólo el 29% de los no CEO está de acuerdo, en cambio; en Latinoamérica la cifra fue similar, con un 35% para la respuesta de los CEOs y un valor de 31% para los no CEOs.

El 36% de los CEOs encuestados a nivel global asegura que se comunican con confianza con clientes y socios comerciales, mientras que para Latinoamérica esto representó un 52%. En tanto que solo el 30% de los no CEOs globales afirma que los cibernéticos reciben ese tipo de apoyo. Para Latinoamérica el valor fue del 40%.

El compromiso y el apoyo del CEO tiene una importancia a largo plazo. Los ejecutivos de la mayoría de las regiones e industrias afirman que para alcanzar una sociedad digital más segura para 2030 es clave educar a los directores y directorios para que puedan cumplir mejor con sus deberes y responsabilidades en torno a la ciberseguridad.

Es hora de cerrar la brecha de expectativas entre los directores ejecutivos y el resto de la C-suite con respecto al nivel de participación de los directores ejecutivos y el apoyo a la ciberseguridad. Las cosas parecen ir en la dirección correcta: las interacciones con el CEO en asuntos cibernéticos han aumentado significativamente en los últimos dos años, según el 46% de los encuestados a nivel global. En cambio, en Latinoamérica arrojó un valor de 55% y en Argentina del 50%.

GRÁFICO 3

¿En cuál de los siguientes asuntos cibernéticos y de privacidad, usted o su CEO estarían personalmente involucrados? Clasifíquelos en orden.

Los CEOs y otros ejecutivos están de acuerdo en los cambios de la misión cibernética

Cuando se les preguntó cómo los CEOs enmarcan la misión de ciberseguridad en su organización, más de la mitad (54%) a nivel global eligió objetivos más amplios y relacionados con el crecimiento de su equipo de seguridad a corto plazo. Respecto a Latinoamérica este valor fue del 51%.

En su mayoría los encuestados coincidieron que la misión principal de la ciberseguridad es: “una forma de establecer la confianza con nuestros clientes con respecto a cómo usamos sus datos de manera ética y protegemos su información”.

Tanto CEOs como no CEOs enumeran objetivos claves similares en cuanto a temas de ciberseguridad en los próximos tres años. Estos objetivos reflejan la famosa jerarquía de necesidades de Maslow, con la prevención como base, o lo más importante; la resiliencia viene a continuación; seguida de la confianza (incluida la confianza del consumidor: “mejor experiencia del cliente” y “mayor lealtad del cliente” ocupan el quinto y séptimo lugar, respectivamente). La protección, la resiliencia y la confianza comprenden las tres claves de la ciberseguridad, cada una de las cuales es importante para la seguridad de la empresa en general.

En resumen

Para el CEO

- Considerar la ciberseguridad como algo importante para el crecimiento empresarial y la confianza del cliente, no solo para establecer mecanismos de defensa y controles, sino también para crear una mentalidad de seguridad en toda la organización.
- Demostrar su confianza y su apoyo al CISO.
- Hacer frente a los problemas y riesgos del modelo de negocio y cambiar lo que sea necesario.

Para el CISO

- Familiarizarse con la estrategia comercial de la organización
- Construir una relación más sólida con el CEO y mantener un diálogo con él y ayudarlo a despejar el camino para prácticas seguras.
- Capacitarse y expandir las habilidades, acorde al rol de ciberseguridad para los negocios. Reorientar al equipo de trabajo hacia el valor comercial y la confianza del cliente.

¿Es tu compañía demasiado compleja para ser asegurada?

Las ventajas de la simplificación

A medida que las conexiones digitales se multiplican, se forman redes cada vez más complejas y sofisticadas. Tener un teléfono inteligente nos permite llevar varios "dispositivos" (teléfono, cámara, calendario, monitor de salud, una biblioteca digital y mucho más) en nuestro bolsillo, simplificando nuestras vidas de muchas maneras.

Pero los procesos necesarios para administrar y mantener todas estas conexiones, incluida la ciberseguridad, también se están volviendo más complejos. Entonces nos preguntamos, ¿Son las compañías demasiado complejas para asegurarlas? Aproximadamente, el 75% del total de los encuestados afirma que hay “demasiada complejidad operativa” innecesaria y evitable, que plantea riesgos cibernéticos y de privacidad "preocupantes". De forma similar, en Latinoamérica arrojó un valor aproximado del 68% mientras que para Argentina fue del 63%.

La infraestructura de datos y las arquitecturas tecnológicas son algunos de los principales factores que más contribuyen a esta complejidad. Para los entrevistados, esta circunstancia se traduce en pérdidas económicas, menor capacidad de innovación y menor capacidad de recuperación ante ciberataques o fallas tecnológicas.

Debido a que algunas complejidades son necesarias, la empresa debe optimizar y simplificar sus operaciones y procesos de manera consciente y enfocarse primero en simplificar donde los beneficios son mayores para toda la organización.

El costo de la complejidad

La complejidad en sí misma no es mala, de hecho, suele ser inherente al crecimiento del negocio, al necesitar más personas y más tecnología. El costo que implica una complejidad innecesaria no es evidente hasta que se produce un ataque.

Principales consecuencias de la complejidad operativa:

- Pérdidas financieras debidas a robo de datos o ciberataques.
- Incapacidad de innovar al ritmo del mercado.
- Falta de resistencia operativa o capacidad de recuperación ante un ciberataque o una falla tecnológica.

El paso a la simplificación

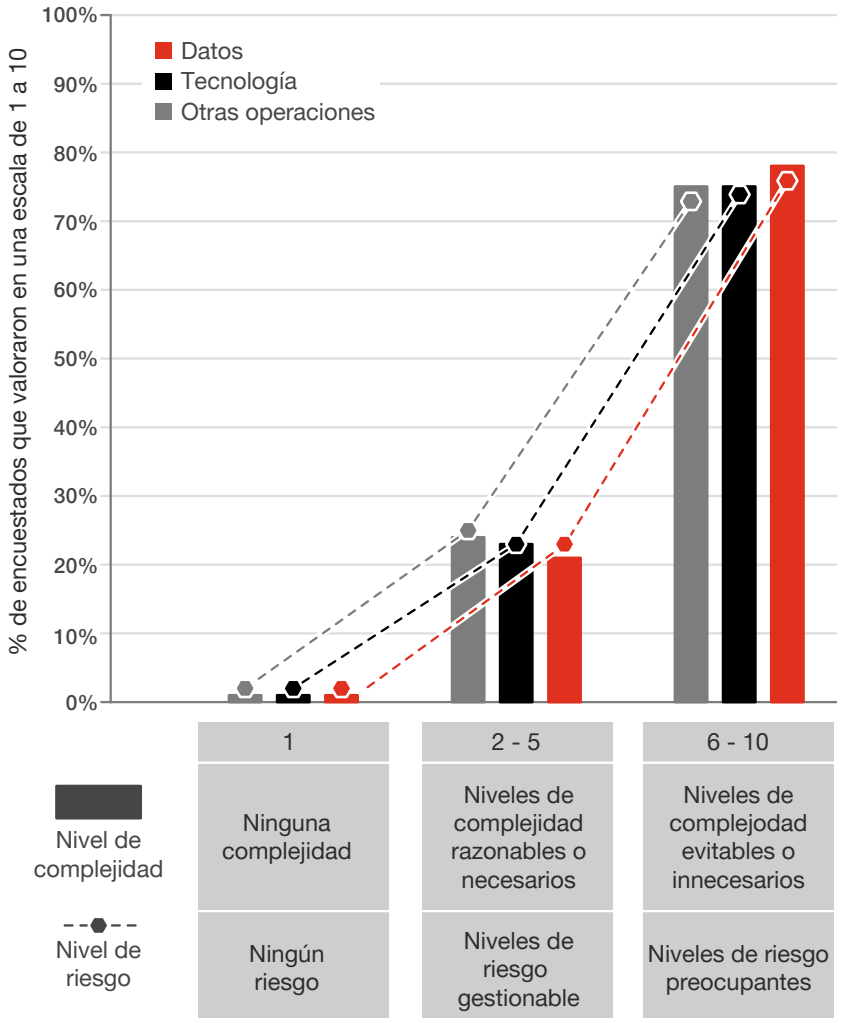
Las empresas que manifiestan haber abordado procesos de simplificación en su organización, se han centrado en consolidar a los proveedores de tecnología y de reajustar la combinación de servicios internos y gestionados, reorganizar las funciones y las formas de trabajo y crear un marco de gobierno del dato integral.

Además, cada vez son más los CISO y CIO que analizan detenidamente sus inversiones, para tratar de consolidar a sus proveedores de tecnología y aplicaciones y revertir, así, el entramado de software y tecnologías diferentes que dificultan su gestión, haciéndolo más vulnerable.

Por último, el paso a la nube puede ayudar a simplificar los procesos de negocio y la arquitectura IT, proporcionar flexibilidad y acelerar la innovación. Si se hace bien, las transformaciones en la nube pueden ser seguras, eficientes y exitosas.

GRÁFICO 4

Nivel de complejidad percibido en las empresas



¿Tu organización está protegida contra los principales riesgos?

Evaluar las oportunidades en base a datos confiables

Los líderes reconocen la importancia de verificar y salvaguardar su información comercial. Cuando se les preguntó acerca de cuál es la misión de la ciberseguridad, la mayoría coincidió en que es una forma de establecer confianza con los clientes con respecto a cómo usamos y protegemos sus datos de forma ética.

No obstante, la complejidad de los datos puede obstaculizar la capacidad de cualquier organización para utilizar eficazmente la información que recopila y genera. La infraestructura y gobierno de datos se clasifican como los dos aspectos más complejos y a su vez innecesarios de las operaciones comerciales. Aproximadamente tres cuartas partes afirma que la complejidad en estas áreas plantea preocupaciones y riesgos para la ciberseguridad y la privacidad.

El primer paso para las organizaciones es establecer una buena base que llamamos confianza en los datos: asegurarse que sean precisos, verificables y seguros para la toma de decisiones comerciales.

Solo alrededor de un tercio de los encuestados, tanto a nivel global como en Latinoamérica, informa tener procesos de confianza de datos maduros y completamente implementados en cuatro áreas clave: gobierno de datos, descubrimiento, protección y minimización. De lo contrario, casi una cuarta parte de nuestros encuestados afirma que no cuenta con ningún proceso formal de confianza en los datos.

Asegurar los datos contra la manipulación y el robo también es fundamental para el éxito, sin embargo, solo alrededor de un tercio de los encuestados informa haber implementado procesos formales de seguridad de datos, que incluyen el cifrado y el intercambio seguro (34%). En Latinoamérica corresponde un 37% y en Argentina un 20%.

Los datos son los activos más buscados por los atacantes. Las empresas pueden minimizar los riesgos, utilizando y protegiendo solo aquellos que necesitan, eliminando el resto (borradores, duplicados, datos reemplazados y personales, etc.)

Las dos terceras partes de las organizaciones que no han implementado formalmente prácticas de confianza en los datos podrían estar en riesgo. Una gobierno de datos eficaz no solo es importante para la resiliencia operativa, sino también para el cumplimiento de las regulaciones.

Convertir los datos en verdaderos activos que pueden aumentar los ingresos es uno de los beneficios de una óptima seguridad. Las empresas que implementan estas buenas prácticas operan de manera más eficiente y prestan un mejor servicio a sus clientes.

GRÁFICO 5

Porcentajes de los que dicen haber implementado completamente procesos formales en torno a estas prácticas de confianza de datos.

Utilizar los datos para mejorar la gestión

Menos de uno de cada tres entrevistados afirma haber integrado herramientas de análisis e inteligencia en su modelo operativo de gestión de riesgos. Esto indica que es poco frecuente que las empresas utilicen los datos para una mejor gestión de riesgos cibernéticos.

Estos encuestados obtuvieron el puntaje más bajo en su capacidad para convertir datos en conocimientos para la cuantificación del riesgo en ciberseguridad, el modelado de amenazas, la construcción de escenarios y el análisis predictivo, todas tecnologías críticas para las decisiones inteligentes en ciberseguridad.

Muchas entidades no se benefician de las herramientas y los enfoques de inteligencia avanzada. Los nuevos tipos de datos internos, los datos de nuevas fuentes externas, las nuevas asociaciones de datos y las plataformas de intercambio de información pueden ser fuentes importantes de inteligencia empresarial, pero solo una cuarta parte de los encuestados dice que está obteniendo beneficios de estas herramientas.

Las empresas que estiman un aumento el próximo año en su gasto en ciberseguridad suelen ser las mismas cuyos modelos operativos utilizan inteligencia de negocios y análisis de datos, procedimientos que pueden ayudar a invertir en ciberseguridad de manera inteligente. Los que tienen mayores mejoras (el top 10% en resultados cibernéticos) tienen 18 veces más probabilidades de afirmar que estos enfoques avanzados son parte integral de su modelo operativo.

GRÁFICO 6

Porcentaje que dice que estos son críticos para su modelo operativo actual.

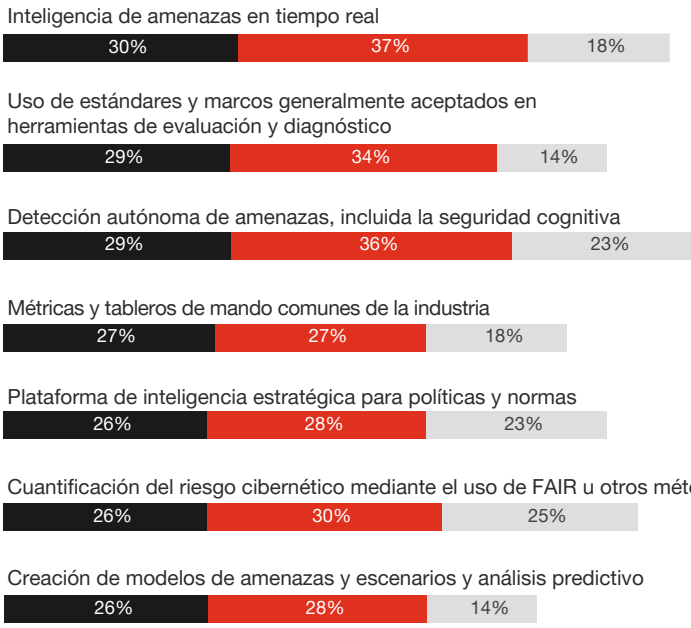
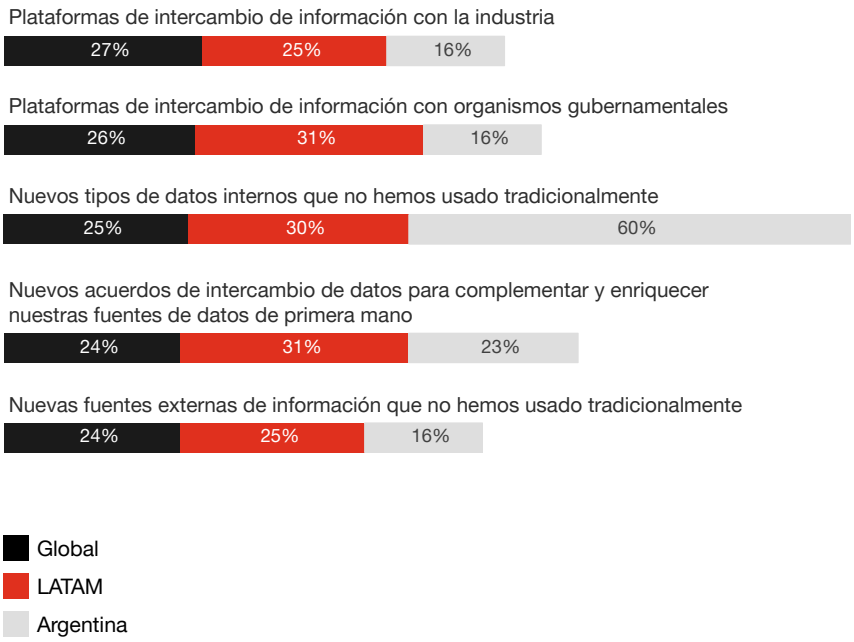


GRÁFICO 7

Porcentaje que informa que se da cuenta de los beneficios de estas herramientas y enfoques



El desafío de evaluar los riesgos en un mundo en constante cambio

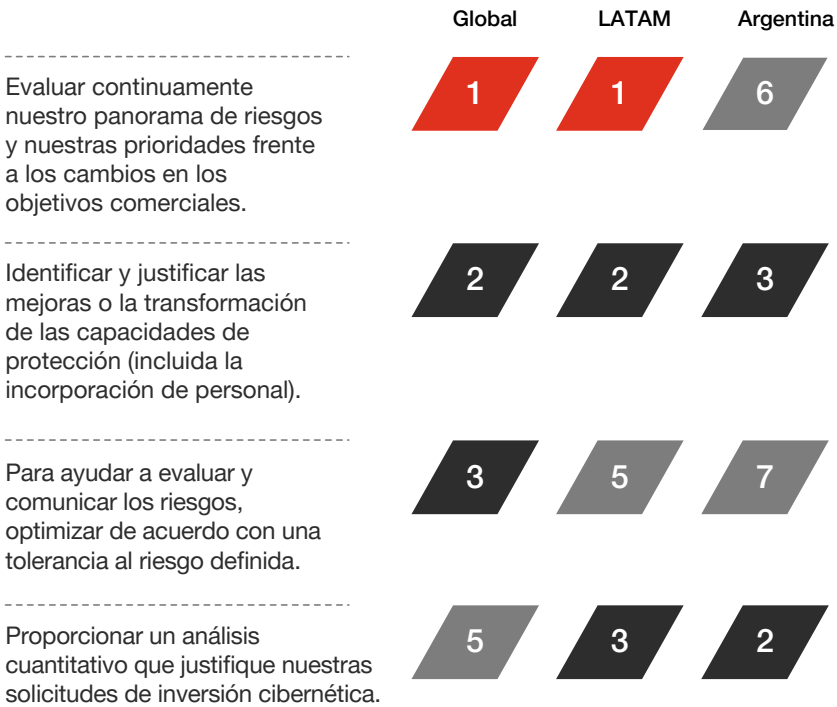
Los líderes reconocen que los riesgos se actualizan y que los datos son la herramienta que les permite monitorearlos y medirlos. En su mayoría coinciden que, para cuantificar el riesgo cibernético, se debería evaluar continuamente las prioridades frente a los objetivos comerciales cambiantes.

Dimensionar los riegos para evaluar las oportunidades y vincular las narrativas de las amenazas cibernéticas con las narrativas comerciales que la alta gerencia y las juntas directivas pueden comprender

Si bien hay un amplio consenso entre las empresas que reconocen la importancia de la ciberseguridad para el modelo de negocios, aún queda un largo camino por recorrer. Entre el 37% y el 42% de los encuestados a nivel global afirma que hay un "progreso significativo" en tanto que para Latinoamérica y Argentina los valores oscilaron entre 36% - 52% y 20%-41% respectivamente. Por su parte hay un registro global entre el 12% y 14% que asegura que se ha logrado poco progreso en la alineación de los objetivos de ciberseguridad y comerciales, mientras que para Latinoamérica el valor fue entre 10% y 13%, y para Argentina entre 5% y 18%.

GRÁFICO 8

Los ejecutivos quieren evaluar los riesgos cibernéticos en un mundo en constante cambio.



Las perspectivas de amenazas para 2022

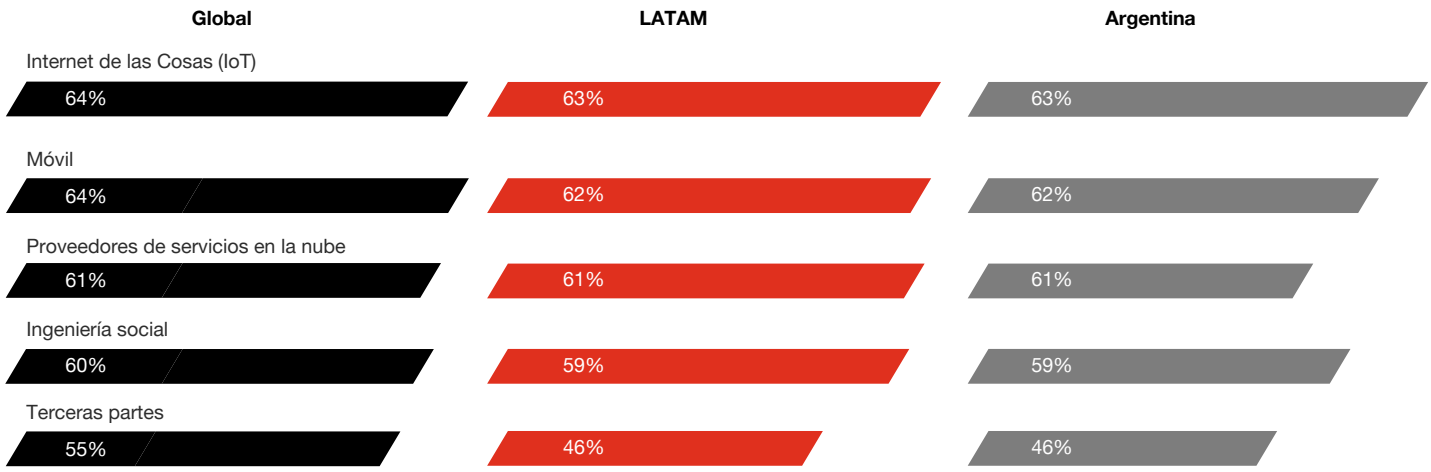
En lo que a amenazas se refiere los participantes plantearon sus perspectivas de cara a los próximos 12 meses, y esperan un aumento en los ataques y los incidentes notificables. El 60% del registro global espera un aumento de los delitos cibernéticos, en cambio, en la región de Latinoamérica y Argentina particularmente coincidieron en un aumento del 52%. Por su parte, el 53% afirma que es probable que aumenten los ataques a los Estado nación. En Latinoamérica arrojó un valor del 51% y en Argentina del 52%. Los dispositivos móviles, Internet de las cosas (IoT) y la nube encabezan la lista de objetivos anticipados.

Los ataques a servicios en la nube (58%) superaron por poco al ransomware (57%) en el contexto global, en tanto que en Latinoamérica los valores fueron de 51% y 47% respectivamente, y para Argentina un 50% en ambos tipos de ataques. La minería de criptomonedas arrojó a nivel global un (54%), ya que es más probable que experimenten aumentos significativos. Para Latinoamérica correspondió un 52% y para Argentina un 48%. Por último, el 56% de los encuestados espera un aumento en las brechas a través de su cadena de suministro de software(global); en tanto que para Latinoamérica y Argentina las cifras fueron de 45% y 32% respectivamente

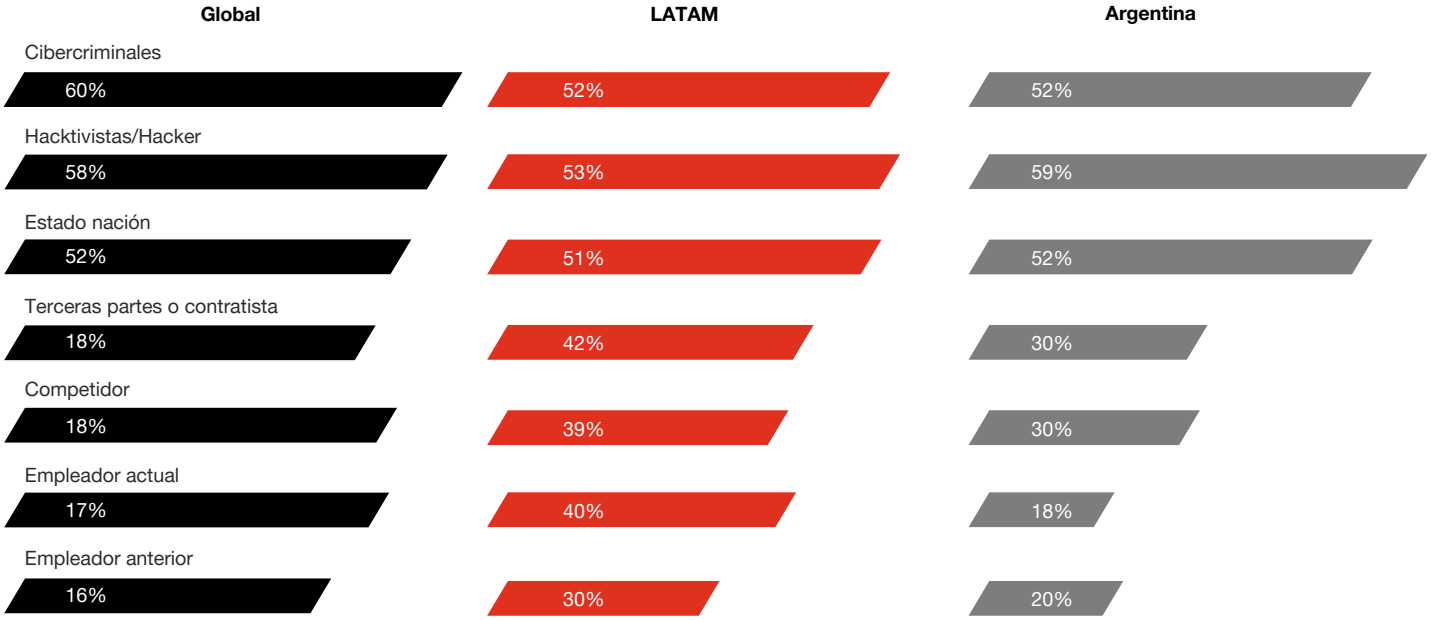
GRÁFICO 9

¿Cómo espera un cambio en los incidentes notificables para estos eventos en su organización? (Respuestas incremento significativo/incremento)

Amenazas a través de vectores



Amenazas a través de actores



En resumen

Para el CFO

Trabajar con el CISO para adoptar un enfoque basado en el riesgo para que el presupuesto cibernético se vincule con los objetivos comerciales.

Para el CISO

- Construir una base sólida de confianza en los datos: un enfoque empresarial para la gestión, el descubrimiento, la protección y la minimización de los datos.
- Crear una hoja de ruta en tiempo real de la cuantificación del riesgo en ciberdelito.
- Con una contabilidad más completa de los riesgos cibernéticos, identificar qué funciona en el modelo de negocio y dónde se necesitar simplificar.

¿Conocés los riesgos que presentan los terceros y la cadena de suministro para tu organización?

Ser conscientes de los peligros que derivan de las relaciones comerciales

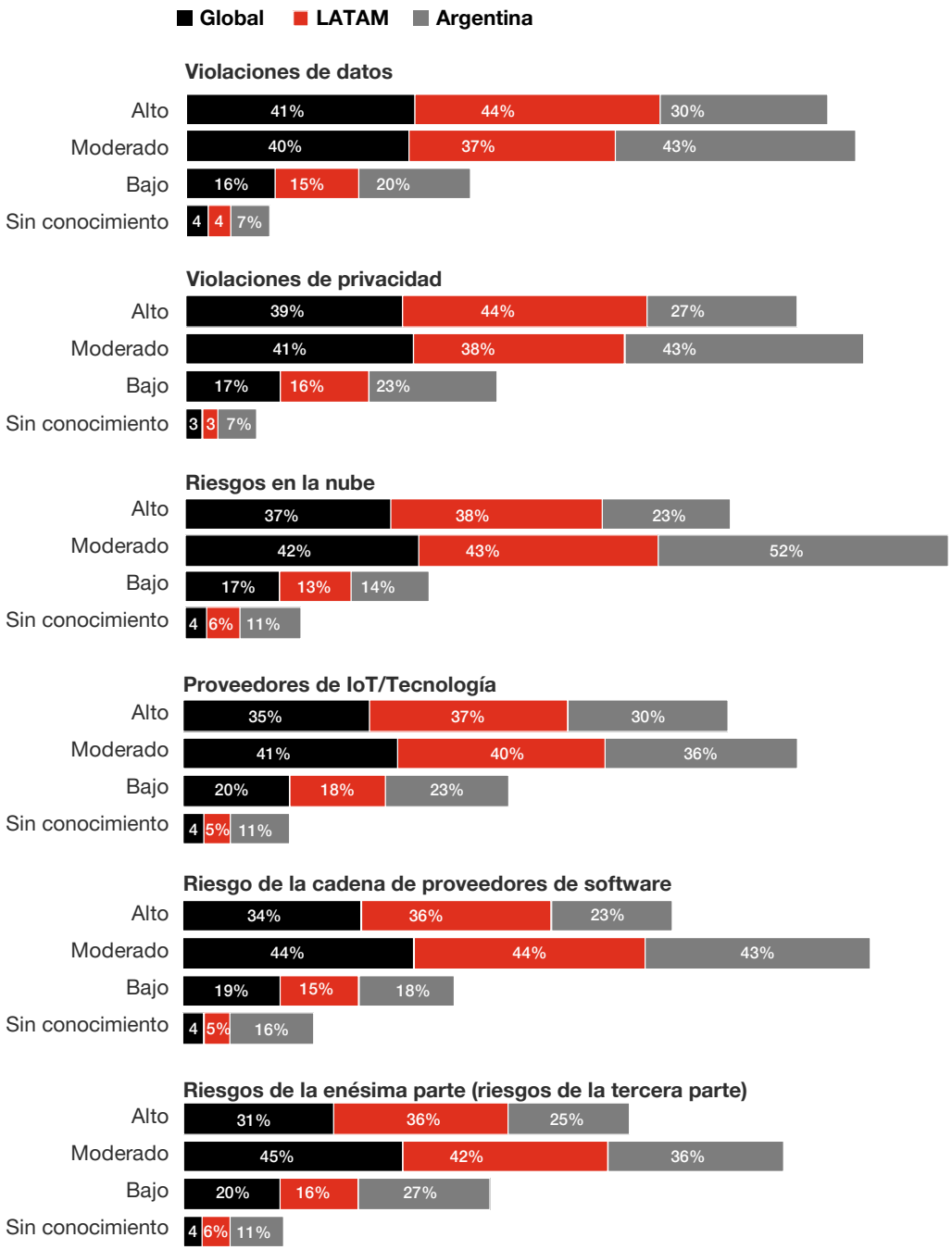
Solo el 40% de los encuestados afirma que comprende a fondo el riesgo de filtraciones de datos a través de terceros, utilizando evaluaciones formales de toda la empresa. En Latinoamérica arrojó un valor de 44% y en Argentina del 30%. Casi una cuarta parte a nivel global tiene poca o ninguna comprensión de todos estos riesgos, un punto débil que los ciberatacantes están dispuestos a explotar.

Por su parte el 56% del registro global espera un aumento en los incidentes notificables en 2022 por ataques a la cadena de suministro de software, en tanto que un 45% corresponde a Latinoamérica y un 32% a Argentina. Sin embargo, solo el 34% de los encuestados a nivel global ha evaluado formalmente la exposición de su empresa a este riesgo, América Latina un 36% y en Argentina es del 23%. El 57% espera un aumento en los ataques a los servicios en la nube, pero solo el 37% manifiesta una comprensión de los riesgos de la nube en base a evaluaciones formales; en cambio en Latinoamérica corresponde un 38% y en Argentina un 23%.

Aproximadamente tres cuartas partes afirman que están muy bien informados sobre los peligros que derivan de terceros. Cuanto más compleja es la conexión, más difícil se vuelve ver los riesgos asociados.

GRÁFICO 10

Las organizaciones tienen un punto débil ante los riesgos que surgen de terceros y de la cadena de suministro



Menos de la mitad de todos los encuestados en el mundo (del 30% al 46%) asegura que han respondido a las crecientes amenazas de los complejos ecosistemas empresariales. En Latinoamérica el rango varía entre el 27% y 56%, mientras que para Argentina va del 23% al 52%.

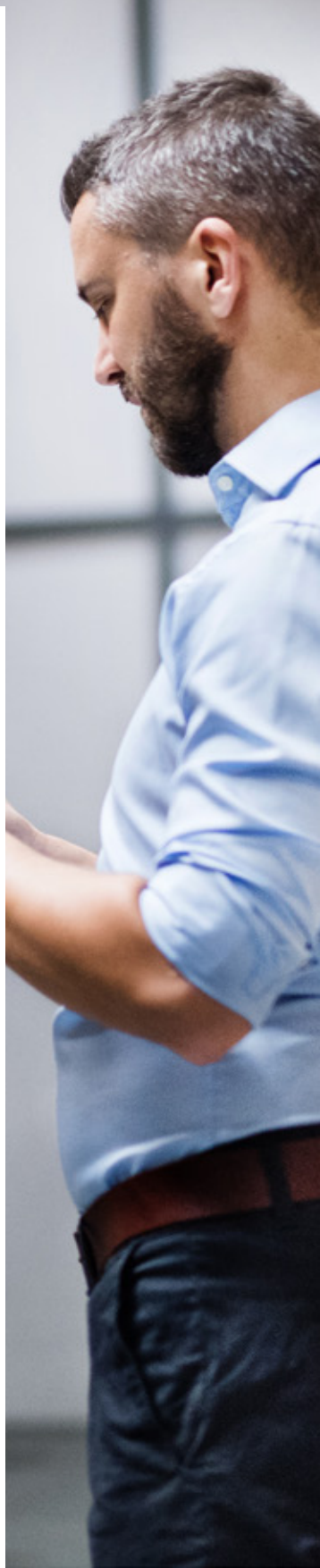
Cuando se les preguntó cómo están minimizando los riesgos de terceros, algunas de las acciones fueron: auditar o verificar el cumplimiento de sus proveedores (46% global, 56% Latinoamérica y 52% en Argentina), compartir información con terceros o ayudarlos de alguna otra manera a mejorar su postura cibernética (42%) a nivel global, en Latinoamérica con un valor del 44% y en Argentina del 36%. Y abordar los desafíos relacionados con el costo o el tiempo para la resiliencia cibernética (40%) a nivel global, en la región de Latinoamérica el 35% y en Argentina del 23%.

Asimismo, más de la mitad no ha tomado ninguna medida que prometa un impacto más duradero en la gestión de riesgos de terceros. No han refinado sus criterios de evaluación de terceros, no han reescrito los contratos (60% global y Latinoamérica, 70% Argentina), no han aumentado el rigor de su debida diligencia (62% global, 59% Latinoamérica y 68% Argentina).

Simplificando la cadena

Una organización podría ser vulnerable a un ataque a la cadena de suministro incluso cuando sus propias ciberdefensas son buenas, y los atacantes simplemente encuentran nuevos caminos hacia la organización a través de sus proveedores. Detectar y detener un ataque basado en software puede ser muy difícil y complejo de desentrañar. Eso es porque cada componente depende de otros como bibliotecas de códigos, paquetes y módulos que se integran en el software y son necesarios para su funcionamiento.

Simplificar el volumen de proveedores de tecnología y otros terceros, así como aumentar su supervisión y ahondar en sus evaluaciones disminuye la complejidad e incrementa la capacidad de conocer el grado de seguridad existente en el esquema de terceros de una empresa.



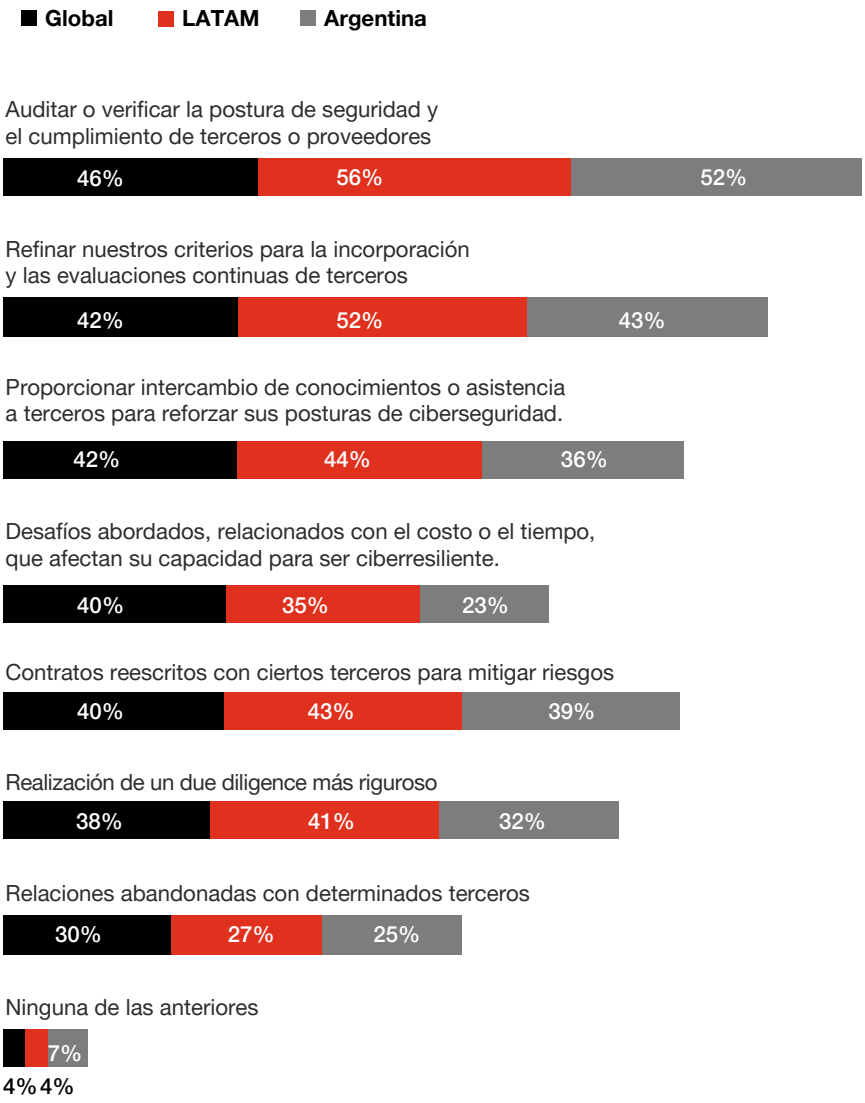
Combinar la tecnología con las terceras partes reduce la complejidad y aumenta su capacidad para saber qué tan seguros son. Un beneficio es que las diferentes funciones (adquisiciones, administradores de riesgos, equipo de fraude, legal, seguridad) pueden comprender mejor sus roles en la protección de sus cadenas de suministro de las interrupciones cibernéticas. Y con menos proveedores que monitorear, su organización puede vigilar de manera más eficiente sus prácticas de seguridad.

Es imprescindible obtener visibilidad en la red de relaciones y dependencias con terceros. Las principales empresas de ciberseguridad integran soluciones (inteligencia de amenazas en tiempo real, búsqueda de amenazas, análisis de seguridad, gestión de vulnerabilidades, detección y respuesta de intrusiones) en amplias plataformas.

Finalmente, los buenos hábitos van de la mano. Los encuestados con prácticas de confianza de datos más avanzadas se destacaron. Redujeron significativamente su número de relaciones con terceros, aumentaron su monitoreo, profundizaron sus evaluaciones de terceros y se sintieron seguros de que su programa de gestión de riesgos de terceros había mostrado beneficios tangibles en los últimos dos años, incluido un mayor ahorro de costos, una implementación más rápida de iniciativas comerciales, mayor confianza del cliente y mayor poder de mercado

GRÁFICO 11

¿Su organización ha realizado alguna de las siguientes acciones en los últimos 12 meses para minimizar los riesgos de terceros o proveedores en su ecosistema?



Colaboración público-privada

La visibilidad también significa ver qué desafíos enfrentan los demás y qué están haciendo al respecto. Los colaboradores pueden ser una parte importante de su ecosistema de negocios cibernéticos.

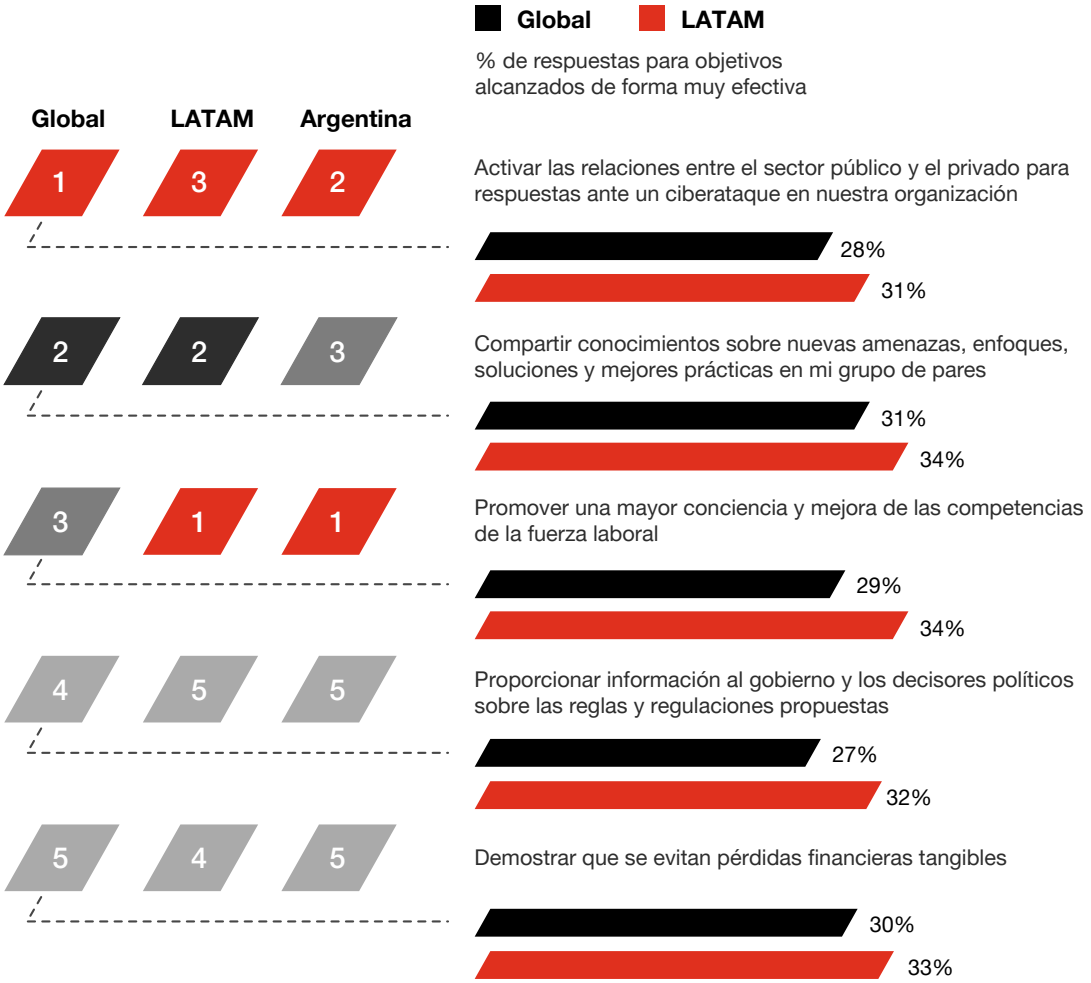
Un tercio de los encuestados expresó que sus esfuerzos de colaboración público-privada los están ayudando "muy eficazmente" a alcanzar sus metas cibernéticas. Sin embargo, aquellos que obtuvieron los mejores resultados de ciberseguridad en los últimos dos años, tenían 34 veces más probabilidades de haber logrado sus objetivos de colaboración público-privada "de manera muy efectiva".

Las organizaciones que aumentaron sus presupuestos cibernéticos en 2022 tenían una probabilidad significativa de decir que habían logrado estos objetivos "de manera muy efectiva":

- Compartir conocimientos sobre nuevas amenazas, enfoques y soluciones en mi grupo de pares (31%) a nivel global mientras que para Latinoamérica es del 34%.
- Demostrar que se evitan pérdidas financieras tangibles (30% global) y 33% para Latinoamérica.
- Activar las relaciones entre el sector público y el privado para obtener respuestas más efectivas a un ciberataque en nuestra organización (28%) global y para Latinoamérica es del 31%.
- Promover una mayor conciencia y mejora de las competencias de la fuerza laboral (29%) global y Latinoamérica un 34%.

GRÁFICO 12

Pensando en su mecanismo de colaboración público-privado más importante, ¿cuáles son los objetivos de su organización con respecto a esta colaboración? Y en el último año, ¿qué tan bien su organización logró cada uno de los objetivos que mencionó?



En resumen

Para el COO y el ejecutivo de la cadena de suministro

- Mapear el sistema y usar un rastreador de terceros para encontrar los eslabones más débiles en su cadena de suministro.
- Examinar a los proveedores de software en función a los estándares de rendimiento que se esperan. El software y las aplicaciones que se utilizan deben someterse al mismo nivel de control que los usuarios y dispositivos de red. El Instituto Nacional de Estándares y Tecnología publicó en julio de 2021, estándares mínimos para las pruebas de software.
- Identificar formas de simplificar las relaciones entre terceros y la cadena de suministro.

Para el CRO y el CISO

- Desarrollar la capacidad tecnológica para detectar y responder a los ataques cibernéticos.
- Establecer una oficina de gestión de riesgos de terceros para coordinar las actividades de todas las funciones que administran las áreas de riesgo.
- Fortalecer los procesos de confianza en los datos.
- Informar a los directorios sobre los riesgos comerciales y cibernéticos de sus terceros, así como de la cadena de suministro.

Acerca de nuestros servicios de seguridad de la información

En PwC Argentina contamos con una práctica que tiene más de 24 años en el mercado, compuesta de profesionales con vasta experiencia y diversidad de conocimientos en materia de seguridad de la información, especializados por industria, plataforma y aplicación.

Contamos además con un laboratorio especialmente diseñado para estudios de seguridad y análisis, así también con un Security Operation Center que permite monitorear eventos de seguridad en forma activa (7x24), y que incorpora inteligencia ante amenazas, detección de vulnerabilidades, y cuando sea requerido, respuesta a incidentes.

Organización: ciberseguridad y seguridad de la información

- Evaluación y diagnóstico del nivel de madurez y estructura organizativa de las áreas.
- Asistencia en la definición y desarrollo del mapa de ruta estratégico de ciberseguridad/seguridad de la información en la organización.
- Evaluación del nivel de cumplimiento en las distintas prácticas y procesos en relación a las mejores prácticas y/o estándares del mercado (NIST, ISO 27000, PCI-DSS, Ley de Protección de los Datos Personales, SWIFT CSP, Normativas del Banco Central, etc.) y asistencia en la alineación a dichas normativas.
- Clasificación de los activos de información.
- Asistencia en la definición y desarrollo de procesos e indicadores de seguridad de la información.

Implementaciones de soluciones de ciberseguridad

- Gestión de identidades y accesos (CIAM y IAM).
- Identidad digital con uso de biómetricas.
- Protección de activos en la nube (Cloud Access Security Broker y seguridad nativa de la nube).
- Implementación de soluciones de Identidad Digital con uso de biométrica.
- Gestión de usuarios privilegiados.
- Implementación de herramientas para la prevención y detección del fraude financiero.
- Detección de vulnerabilidades en redes de Tecnologías de la Operación (OT)
- Gestión de riesgos.
- Implementación de esquemas de seguridad para distintas plataformas y sistemas.
- Diagnóstico de configuración de los sistemas y recomendaciones de mejora.
- Seguridad en redes OT/ICS.
- Análisis de arquitectura de red global.
- Revisión del ciclo de vida del desarrollo de software (SDLC) y desarrollo con metodologías ágiles y DevOps.

Pruebas de intrusión

- Red externa (modalidad caja negra).
- Red interna (modalidad caja gris).
- Red inalámbrica.
- Detección de redes inalámbricas (WiFi) con el fin de identificar el inventario de la compañía. A su vez, analizar el nivel de cifrado de seguridad y protección de las redes en uso por parte de la organización.
- Ingeniería social
- Ejercicios Red Team - OSINT

Ingeniería social

- Phishing SCAM.
- Acceso físico.
- Naiting.
- Ingeniería social reversa.
- Pharming.
- Vishing.

Ciberinteligencia

- Monitoreo 7x24 sobre los activos críticos del negocio, para la detección de:
  - Fugas de información.
  - Robo de credenciales.
  - Hacktivismo, activismo en la red y ataques DDoS.
  - Exposición/vulneración.
  - Uso no autorizado de marca, logo o imagen.
  - Seguimiento de dominios.
  - Seguimiento de identidad digital.
  - Protocolos de actuación.
  - Amenazas sectoriales.
  - Amenazas socio-culturales.

Security Operations Center (SOC)

- Servicio de monitoreo de eventos de seguridad que funciona las 24 horas y permite alertar amenazas cibernéticas.
- Dentro de las actividades se incluyen:
  - Inventario de activos.
  - Evaluación de vulnerabilidades.
  - Monitoreo de comportamiento.
  - Detección de intrusos.
  - Security Information Event Management (SIEM).
  - Inteligencia ante amenazas.

Investigación forense

- Adquisición de evidencia (equipos físicos, tráfico de red, documentos, email, dispositivos móviles, mensajería instantánea, otros).
- Investigación de comunicaciones.
- Definición de palabras clave asociada con la investigación.

Respuesta a incidentes:

- Definir las acciones precisas para el monitoreo y control;
- Atención y recepción de eventos o potenciales incidentes;
- Proceso de notificación y escalamiento;
- Resolución y acciones pos-incidente.
- Asistencia en la gestión de la ciber-crisis: cuantificación de impacto del ataque, afectación de contratos con terceros y SLAs, incumplimiento de normativas, cómunicaciones a terceras partes y/o prensa, etc.

Desarrollo de procedimientos de gestión de cibercrisis

- Desarrollo de procesos integrales para la gestión de cibercrisis que permitan establecer las acciones frente a un incidente de seguridad con alto impacto para la organización, alineados a los procedimientos existentes del BCP/DRP.

Plan de continuidad de negocios

- Elaboración de análisis de impacto al negocio y análisis de riesgo.
- Definición de estrategias de continuidad
- Elaboración de procedimientos de recuperación de desastres (DRP).

Entrenamiento y concientización a usuarios

- Preparación y ejecución de capacitaciones, entremientos y actividades de concientización, que tiene como objetivo abordar los riesgos y amenazas que afectan la confidencialidad, integridad y disponibilidad de la información, así como las medidas de protección relacionadas.

Gobernabilidad, riesgo y cumplimiento (GRC)

- Implementación de seguridad SAP.
- Assessment y reingeniería de seguridad SAP.
- Implementación de matriz de segregación de funciones.
- Outsourcing de seguridad SAP.
- Implementación de sistemas GRC.

Acerca de la encuesta

La encuesta Global Digital Trust Insights 2022 (antes Encuesta Global de Seguridad de la Información (GISS) fue realizada por PwC en julio y agosto de 2021. Los resultados analizados en este informe se basan en las respuestas de 3.602 ejecutivos de negocios, tecnología y seguridad (CEO, CFO, CISO y CIO) en 66 países.

El 62% de los encuestados son ejecutivos de empresas grandes (us$ 1.000 millones o más en ingresos). El 33% pertenece a empresas con ingresos de us$ 10.000 millones o más.

Los participantes pertenecen a diferentes industrias: tecnología, medios, telecomunicaciones (23%), mercados minoristas y de consumo (16%), servicios financieros (20%), manufactura industrial (22%), energía (8%), salud (7%) y servicios públicos (3%).

Un 33% proviene de Europa Occidental, un 26% de América del Norte, un 18% de Asia Pacífico, un 10% de América Latina, un 4% de Europa del Este y un 4% de Medio Oriente.

Más información en https://www.pwc.com/dti2022

Contactos

Enzo Taibi
Socio de PwC Argentina

enzo.i.taibi@pwc.com
/enzo-taibi

Diego Taich
Managing Director de PwC Argentina

diego.taich@pwc.com
/diego-taich