Informe El futuro del trabajo remoto seguro

cisco SECURE

RESUMEN EJECUTIVO

La pandemia de COVID-19 ha provocado que las empresas de todo el mundo hagan la transición a un entorno de trabajo remoto a una velocidad y escala sin precedentes. Lo que alguna vez fue una modalidad opcional para los empleados y las empresas se convirtió en algo imprescindible casi de la noche a la mañana: organizaciones de todo el mundo han implementado acuerdos de trabajo remoto para toda su fuerza laboral. A medida que sucedía la transición, las organizaciones tuvieron que adaptar y desarrollar sus enfoques, soluciones y políticas de ciberseguridad para que los empleados pudieran trabajar de forma remota, acceder a los recursos de la empresa de manera segura y garantizar la continuidad del negocio.

En lo que ha sido un año cargado de incertidumbre, ha surgido una tendencia importante: la de un futuro laboral flexible e híbrido. Después de haber trabajado de manera remota durante un período prolongado, los empleados ahora esperan tener la flexibilidad y la capacidad para trabajar desde cualquier lugar, en cualquier momento y con cualquier dispositivo, en una era posterior a la COVID, incluso cuando regresen a la oficina.

Esto ha acelerado la necesidad de las empresas de reevaluar su postura en materia de ciberseguridad, especialmente en este momento en el que los líderes empresariales buscan desarrollar empresas resilientes. La seguridad puede ser el puente hacia la resiliencia empresarial, ya que permite que las empresas operen con flexibilidad mediante una adaptación segura, con el fin de brindar protección tanto en el presente como en el futuro. Para lograrlo, es clave garantizar que las soluciones de red y colaboración sean flexibles, fáciles de usar, eficaces y seguras, tanto en los centros de datos en las instalaciones o en la nube, como en todos los dispositivos de los usuarios, ya sean de trabajo o personales.

Queríamos comprender cuál era el nivel de preparación de las organizaciones para proteger su negocio, en diferentes partes del mundo, ya que se vieron obligadas a pasar toda la fuerza laboral a la modalidad remota debido a la pandemia. Más importante aún, queríamos obtener información sobre cuál es la situación de las organizaciones hoy en día en relación con el aumento de las amenazas y alertas de ciberseguridad, los desafíos que enfrentaron en esta transición repentina y cómo están adaptando sus enfoques en materia de ciberseguridad a fin de estar mejor preparadas para el entorno de trabajo híbrido y flexible, que llegó para quedarse. Para ello, encargamos una encuesta de investigación global en 21 mercados de América (AMER), Asia Pacífico, Japón y China (APJC), y Europa, para encuestar a más de 3000 responsables de la toma de decisiones de TI, desde pequeñas empresas hasta grandes compañías.

El estudio, titulado " El futuro del trabajo remoto seguro" , tiene como objetivo comprender mejor los desafíos que enfrentan las organizaciones en la transición al trabajo remoto, además de revelar el estado de su preparación en ciberseguridad y los cambios en sus prioridades, políticas e inversiones a medida que se preparan para un entorno de trabajo híbrido que probablemente sea la norma de ahora en más.

Los resultados son reveladores.

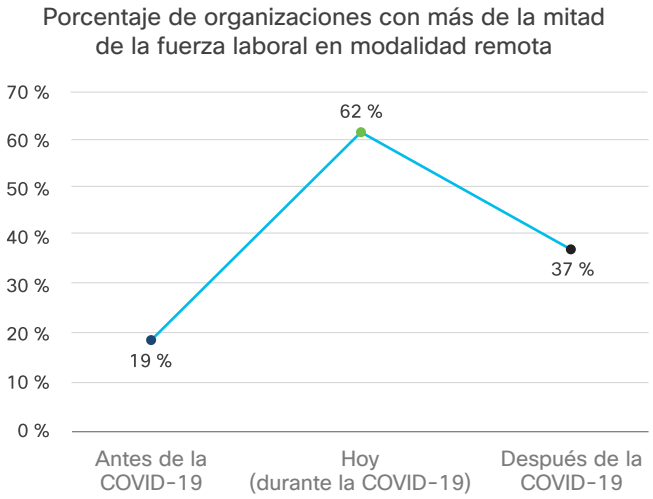
RESULTADOS GLOBALES

RESULTADOS GLOBALES

La importancia de la ciberseguridad en un futuro laboral híbrido

Las organizaciones no regresarán al estado previo a la COVID-19

Las organizaciones comienzan a prepararse para un mundo posterior a la pandemia y una cosa está quedando clara: ahora los empleados esperan disponer de la flexibilidad y la capacidad para trabajar de forma remota, independientemente de lo que implique el futuro del trabajo, dado que no volveremos a como eran las cosas antes de la COVID-19. Como se observó de manera uniforme en las tres regiones, el trabajo remoto aumentó a niveles sin precedentes cuando comenzó la pandemia en marzo; dos tercios (62 %) de los encuestados tenían ***más de la mitad de la fuerza laboral*** trabajando desde su casa. El 37 % de los encuestados afirmó que ***más de la mitad de su fuerza laboral*** desea seguir trabajando desde la casa después de la pandemia, en comparación con el 19 % antes de que la enfermedad tomara el mundo por sorpresa.



Porcentaje de encuestados con más de la mitad de su fuerza laboral en modalidad remota

	Global	APJC	AMER	Europa
Antes de la COVID-19	19 %	19 %	24 %	16 %
Hoy (durante la COVID-19)	62 %	56 %	75 %	67 %
Después de la COVID-19	37 %	34 %	46 %	34 %

Las organizaciones del mercado de América ocupan el primer puesto: el 75 % de los encuestados tiene ***más de la mitad*** de su fuerza laboral trabajando de forma remota en este momento. Las siguen las empresas de Europa con el 67 % y de APJC con el 56 %.

Sin embargo, no volverán a los niveles previos a la pandemia en el corto plazo, ya que el 46 % de los encuestados del mercado de América espera que más de la mitad de sus empleados continúen trabajando en forma remota, incluso después de que las empresas hayan vuelto a la normalidad. De manera similar, el 34 % de los encuestados de APJC y Europa observó lo mismo.

Las actitudes respecto del trabajo remoto también son uniformes en las organizaciones pequeñas, medianas y grandes: el 35 % de las pequeñas empresas, el 38 % de las empresas medianas y el 37 % de las grandes empresas creen que ***más de la mitad*** de sus empleados serán trabajadores remotos después de la COVID-19.

Si bien es probable que muchas empresas aún no sepan con certeza cómo será el futuro del trabajo, contar con la flexibilidad para adaptarse de manera segura a la situación presente y a la que se viene aumentará su resiliencia empresarial y les permitirá contar con una fuerza laboral más distribuida.

Algunos países más que otros planean adoptar el trabajo remoto de aquí en más

Curiosamente, si bien el plan de la mayoría de las organizaciones es que la mayor parte de los empleados regrese a la oficina después de la pandemia, algunos países se oponen a la tendencia: una mayor proporción de encuestados afirmó que ***más de la mitad*** de la fuerza laboral de su organización seguirá estando formada por trabajadores remotos en el futuro. Estos incluyen el 48 % en Filipinas y el 50 % en el Reino Unido y los Estados Unidos, así como el 53 % en Brasil e India, todos los cuales superan el promedio global del 37 %.

48 %
Filipinas

53 %
Brasil
India

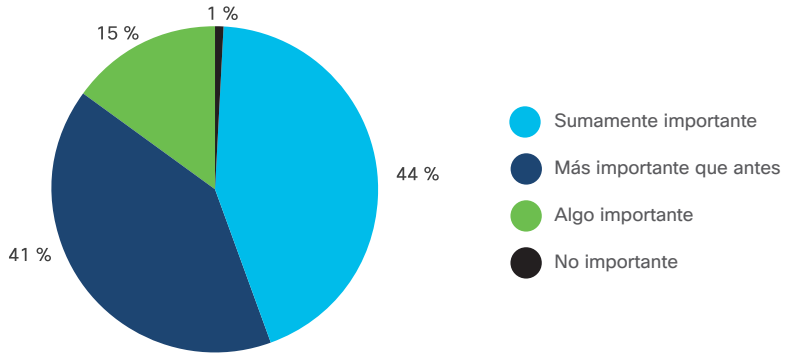
50 %
Reino Unido
Estados Unidos

Para hacer posible este futuro flexible e híbrido de la tendencia laboral, las empresas necesitan una infraestructura subyacente segura sin fisuras.

Ahora, la ciberseguridad es la prioridad corporativa principal

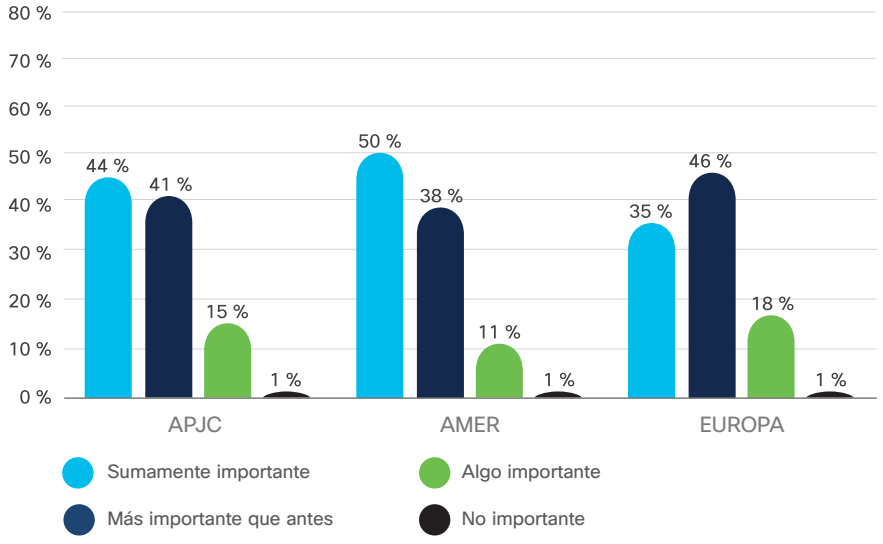
La buena noticia es que la ciberseguridad se ha convertido en una de las mayores prioridades para las organizaciones. El 85 % de los encuestados de todo el mundo afirmó que la ciberseguridad es *sumamente importante* o *más importante* **que antes de la pandemia.**

Porcentaje global de la importancia de la ciberseguridad



Más específicamente, una gran parte de los encuestados de APJC (44 %) y América (50 %) afirmó que la ciberseguridad es ***sumamente importante*** para su negocio. Europa, por otro lado, presentó más encuestados que indicaron que es ***más importante que antes*** (46 %).

Importancia de la ciberseguridad por región



Esta tendencia también es uniforme en las empresas pequeñas, medianas y grandes, con un **79 %, 87 % y 88 %,** respectivamente.

	Pequeña	Medio	Grande
Sumamente importante	36 %	42 %	53 %
Más importante que antes	44 %	45 %	35 %
Algo importante	19 %	13 %	11 %
No importante	1 %	1 %	0 %

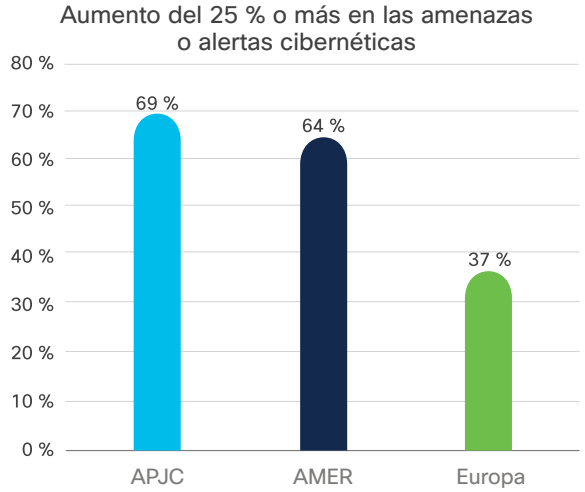
Importancia de la ciberseguridad por tamaño de la organización

Un repunte resiliente: abordar las amenazas y los desafíos en materia de ciberseguridad

Aumento de las alertas y las amenazas cibernéticas en diversos niveles

En todo el mundo, las empresas experimentaron un salto en la cantidad de amenazas o alertas de ciberseguridad durante la pandemia, ya que los agentes maliciosos intentaron aprovechar las posibles brechas de seguridad que se producen cuando los usuarios acceden a la red corporativa y las aplicaciones en la nube de forma remota. El 61 % de los encuestados de todo el mundo afirmó que sus organizaciones experimentaron un salto del ***25 % o más en la cantidad de amenazas o alertas cibernéticas*** desde el comienzo de la pandemia de COVID-19. Esto también se presentó en el 55 % de las pequeñas empresas, el 70 % de las organizaciones medianas y el 60 % de las grandes compañías.

Con un 69 %, fueron más los encuestados de APJC que experimentaron un salto del ***25 % o más en la cantidad de amenazas o alertas cibernéticas*** desde el surgimiento de la COVID-19. A esto le sigue el 64 % en América y el 37 % en Europa.



De manera preocupante, el 8 % de las empresas de todo el mundo no sabe si han experimentado un aumento o una disminución de las amenazas cibernéticas. Esta cifra es del 17 % para los encuestados de Europa, en comparación con el 6 % de APJC y el 5 % de América. Al profundizar, vemos que el estudio también reveló algunas diferencias clave entre los niveles de amenazas o alertas que se presentan en los diferentes sectores y regiones.

Porcentaje de aumento de amenazas o alertas cibernéticas	Global	APJC	AMER	Europa
0 % al 24 %	31 %	25 %	31 %	47 %
25 % al 50 %	33 %	35 %	36 %	23 %
51 % al 75 %	23 %	27 %	24 %	11 %
76 % al 100 %	5 %	6 %	3 %	2 %
No lo sé	8 %	6 %	5 %	17 %

25 % o más en amenazas

Porcentaje de aumento de amenazas o alertas cibernéticas

Por ejemplo, el 78 % de las organizaciones del sector de **arquitectura e ingeniería** experimentó un aumento del 25 % o más en la cantidad de amenazas o alertas cibernéticas, la cifra más alta de todos los sectores. A esto le siguen el sector de la **fabricación e ingeniería química** con un 72 % y el sector de la **educación** con un 70 %.

Curiosamente, los sectores que a menudo se consideran de mayor interés para los atacantes, como los **servicios financieros** (58 %), el **desarrollo de software** (62 %) y los **servicios de salud** (54 %), desafiaron las expectativas con una proporción relativamente menor de organizaciones que registraron más alertas.

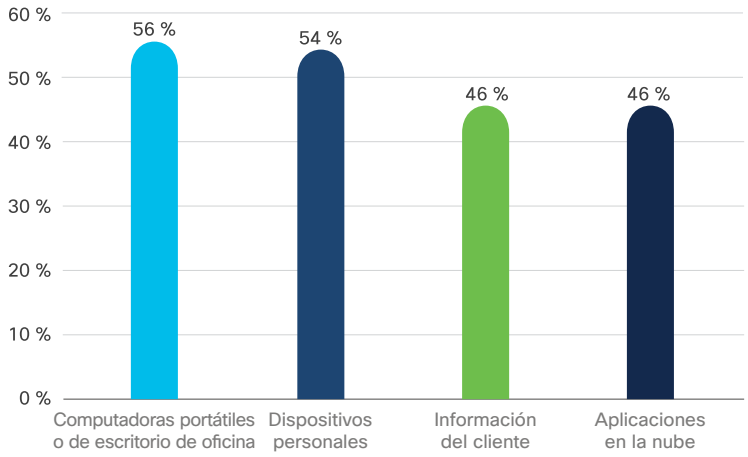
Principales desafíos de ciberseguridad de las organizaciones que permiten el trabajo remoto

El acceso seguro, definido como la capacidad de habilitar de manera segura el acceso a la red empresarial y las aplicaciones para cualquier usuario, desde cualquier dispositivo y en cualquier momento, es el ***principal desafío de ciberseguridad*** al que se enfrenta la mayor parte de las organizaciones (62 %) que tienen trabajadores remotos. Otras inquietudes planteadas por las organizaciones de todo el mundo incluyen la privacidad de los datos (55 %), que tiene implicaciones para la postura general en materia de seguridad, y el mantenimiento del control y la aplicación de políticas (50 %).

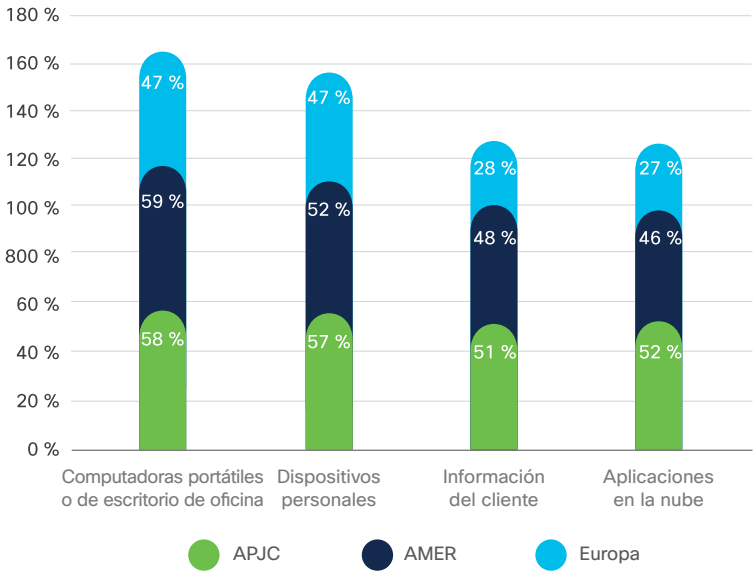
Protección de una cantidad cada vez mayor de terminales

La protección de dispositivos es un desafío cada vez mayor para las organizaciones, que ahora no pueden depender de la conexión de los terminales a las redes del campus para obtener visibilidad y aplicar actualizaciones. Al mismo tiempo, los empleados se conectan a los recursos corporativos con dispositivos más personales, no administrados, lo que constituye un punto ciego para los equipos de seguridad. Uno de cada dos encuestados indicó que las computadoras portátiles o de escritorio de las oficinas (56 %) y los dispositivos personales (54 %) son difíciles de proteger en un entorno remoto. Otras áreas que presentan esta dificultad son la información de los clientes y las aplicaciones en la nube, ambas con un 46 %.

Aspectos que fueron difíciles de proteger en un entorno remoto



Comparación regional de los aspectos que fueron difíciles de proteger en un entorno remoto

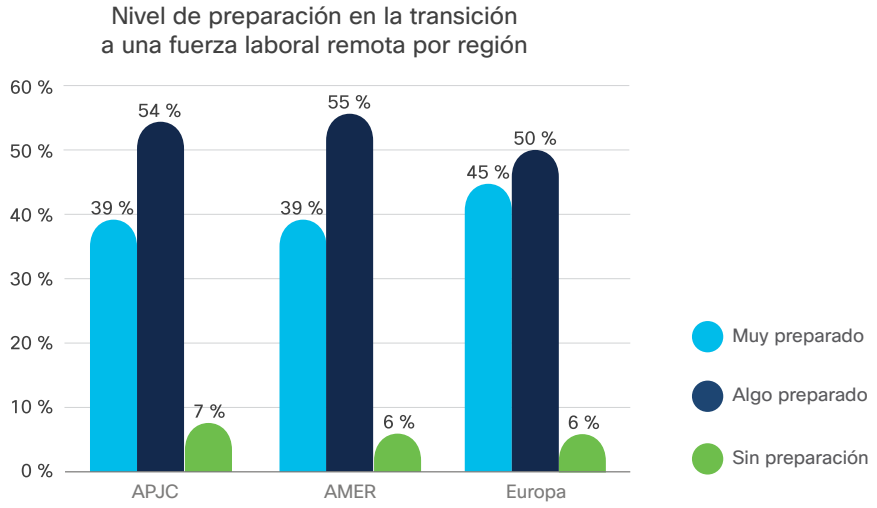


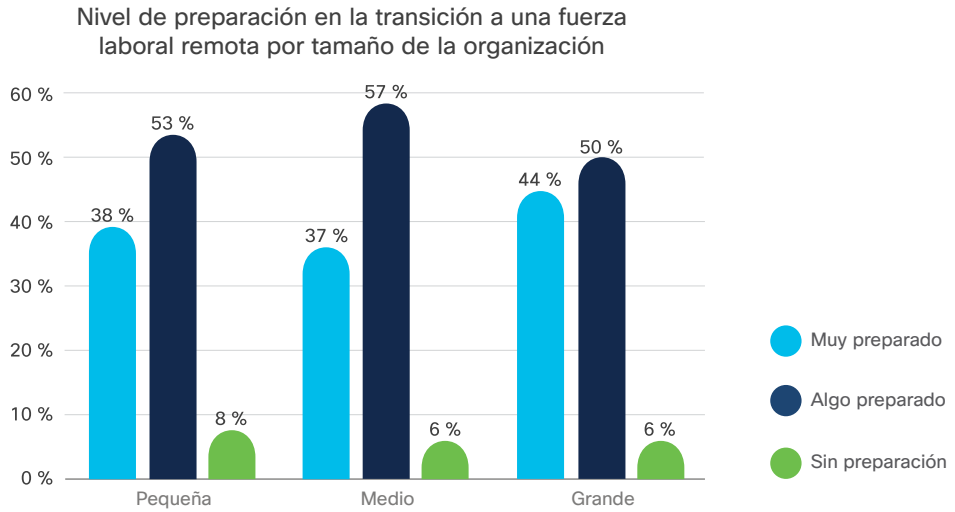
Las organizaciones se ven obligadas a acelerar la transformación digital

Si bien muchas organizaciones habían comenzado la transición para darle prioridad a la nube y a la modalidad remota incluso antes de la pandemia, se trata de un proceso que requiere mucho tiempo e inversión. Prácticamente de la noche a la mañana, la fuerza laboral de muchas organizaciones pasó a estar distribuida; esto puso en evidencia cuál era su nivel de preparación para ello. En todo el mundo, los encuestados indicaron que contaban con ***algo de preparación*** (53 %) o que ***no estaban preparados*** (6 %) para acelerar la transición a un entorno de trabajo remoto cuando comenzó la pandemia de COVID-19.

	Global	APJC	AMER	Europa
Muy preparado	40 %	39 %	39 %	45 %
Algo preparado	53 %	54 %	55 %	50 %
Sin preparación	6 %	7 %	6 %	6 %

Nivel de preparación en la transición a una fuerza laboral remota





En cuanto a los sectores específicos, las organizaciones del sector de **arquitectura e ingeniería** (72 %) presentó la mayor cantidad de encuestados que estaban ***algo preparados***, más que el promedio global del 53 %, mientras que los siguientes sectores presentaron la mayor proporción de encuestados que ***no estaban preparados*** para la transición repentina en comparación con el promedio global del 6 %: **comercio mayorista y distribución** (15 %); **educación** (14 %); y **fabricación e ingeniería química**, **fabricación no relacionada con la informática** y **organizaciones de beneficencia o sin fines de lucro** (10 %, respectivamente).

La preparación (o no) de los equipos de seguridad y de TI para permitir el trabajo remoto refleja potencialmente la naturaleza de las empresas y la capacidad de los trabajadores de ese sector para dedicar parte o la totalidad de su tiempo a las operaciones fuera de la oficina. Las empresas que se inclinan al trabajo con el conocimiento presentan más probabilidades de tener una mayor cantidad de empleados remotos que los sectores específicos de determinadas ubicaciones, como la fabricación. Naturalmente, las empresas con una mayor cantidad de empleados en modalidad de trabajo a distancia estarán más preparadas para que una cantidad aún mayor de su fuerza laboral se vuelva remota.

Del 67 % que indicó estar ***muy preparado***, las organizaciones vietnamitas presentaron la mayor proporción de encuestados del mundo que estaban listos para una transición inmediata al trabajo remoto. Les siguen Reino Unido (59 %), la India (54 %) e Indonesia (49 %).

Por otro lado, Estados Unidos, que tenía la mayor proporción de trabajadores remotos antes de la pandemia (el 32 % tenía más de la mitad de la fuerza laboral en modalidad remota), presentó una mayor proporción de organizaciones que solo estaban ***algo preparadas*** (48 %) en comparación con ***preparadas*** (46 %).

Priorizar la ciberseguridad para el presente y para lo que se viene

Adopción y priorización de la tecnología

La buena noticia es que, de todas las soluciones de tecnología adoptadas para permitir el trabajo remoto, las organizaciones calificaron a las medidas de ciberseguridad como la prioridad número 1 (el 52 % la clasificó en primer lugar). A ella le siguen las herramientas de colaboración (el 41 % las calificó en primer lugar) y los servicios profesionales (el 27 % los calificó en primer lugar).

Lo más adoptado	frente a	La prioridad número 1
Herramientas de colaboración 73 %	1	Medidas de ciberseguridad 52 %
Medidas de ciberseguridad 68 %	2	Herramientas de colaboración 41 %
Uso compartido de documentos en la nube 63 %	3	Servicios profesionales 27 %
Protección de datos distribuidos 49 %	4	Uso compartido de documentos en la nube 22 %
Servicios profesionales 33 %	5	Protección de datos distribuidos 19 %

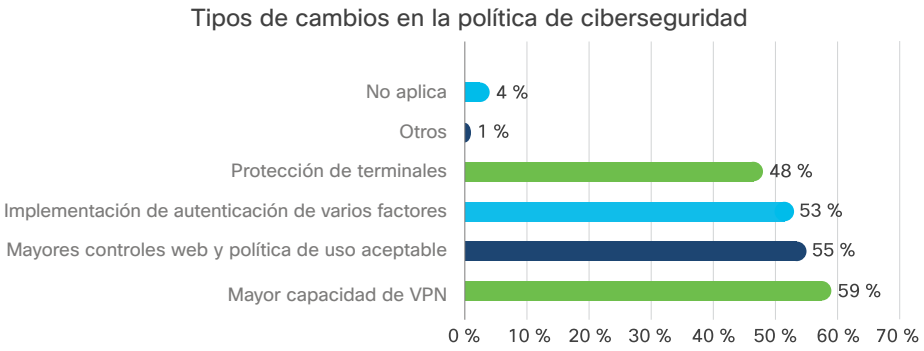
A medida que las empresas se adentran en el futuro del trabajo —lo que probablemente implique la adopción de diversas soluciones, desde la colaboración hasta el intercambio de archivos y las redes—, es fundamental garantizar que la seguridad esté integrada en todas las herramientas de TI. Esto dará verdadero poder a la fuerza laboral segura y distribuida.

Facilitar el trabajo remoto con los protocolos y las políticas correctos

El 96 % de las organizaciones de todo el mundo indicó que ha hecho cambios en las políticas de ciberseguridad para respaldar el trabajo remoto. Estas incluyen el 93 % de las pequeñas empresas, el 98 % de las organizaciones medianas y el 97 % de las grandes organizaciones, lo que indica que las organizaciones de todos los tamaños consideraron absolutamente necesario actualizar sus políticas inmediatamente para respaldar este cambio.

Parece obvio, pero cabe mencionar que, cuando su equipo de RR. HH. o el equipo de finanzas, por ejemplo, se ven repentinamente obligados a trabajar de forma remota, las protecciones y el acceso que se les otorgan como parte de las responsabilidades diarias dentro de la red corporativa deben replicarse para la modalidad remota a fin de permitir la continuidad del negocio. La uniformidad de las políticas también adquiere más complejidad que antes.

En relación con esto, los principales cambios relativos a las políticas fueron el aumento de la capacidad de VPN (59 %), el aumento de los controles web y la política de uso aceptable (55 %), y la implementación de la autenticación de varios factores (MFA, 53 %).



Global	APJC	AMER	Europa
Mayor capacidad de VPN (59 %)	Mayores controles web y política de uso aceptable (61 %)	Mayor capacidad de VPN (64 %)	Mayor capacidad de VPN (64 %)
Mayores controles web y política de uso aceptable (55 %)	Implementación de autenticación de varios factores (59 %)	Mayores controles web y política de uso aceptable (57 %)	Implementación de autenticación de varios factores (38 %)
Implementación de autenticación de varios factores (53 %)	Mayor capacidad de VPN (56 %)	Implementación de autenticación de varios factores (51 %)	Mayores controles web y política de uso aceptable (34 %)

Los 3 principales cambios en las políticas de ciberseguridad por región

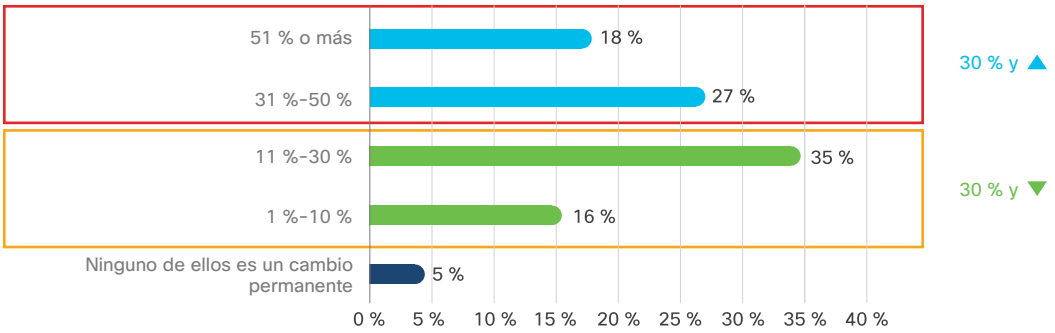
VARIACIONES REGIONALES:

- **Mayores controles web y uso aceptable:**
  - Primer lugar en APJC (61 %)
  - Segundo lugar en AMER (57 %), similar al resultado global (55 %)
  - Tercer lugar en Europa (34 %)
- **Implementación de autenticación de varios factores:**
  - Segundo lugar en APJC (59 %) y en Europa (38 %)
  - Tercer lugar en AMER (51 %)
- **Mayor capacidad de VPN:**
  - Primer lugar en AMER y Europa (ambos 64 %), similar al resultado global (59 %)
  - Tercer lugar en APJC (56 %)

Se están produciendo cambios a largo plazo en las políticas de ciberseguridad corporativa

Una de las mayores observaciones del estudio es que el trabajo remoto está generando cambios a largo plazo en las políticas de ciberseguridad. Esto da a las organizaciones la oportunidad única de transformar sus estrategias comerciales y de seguridad para respaldar verdaderamente el mundo en el que vivimos actualmente, donde lo digital es la prioridad. Esto hace posible el nivel de flexibilidad que esperan ahora los empleados con una fuerza laboral distribuida.

Con este fin, entre las organizaciones que realizaron cambios en las políticas de ciberseguridad, la gran mayoría (95 %) indicó que algunos de ellos son permanentes.



Proporción de cambios realizados en las políticas de ciberseguridad que son permanentes

Una mirada más profunda en todas las regiones revela que más organizaciones en el mercado de América (54 %) y Europa (48 %) afirmaron que ***más del 30 %*** de los cambios en las políticas de ciberseguridad serán permanentes, mientras que el 41 % de los encuestados de APJC indicó lo mismo.

Magnitud de los cambios permanentes en las políticas	Global	APJC	AMER	Europa
30 % o menos	50 %	54 %	44 %	45 %
Más del 30 %	45 %	41 %	54 %	48 %
TOTAL	**95 %**	**96 %**	**97 %**	**93 %**

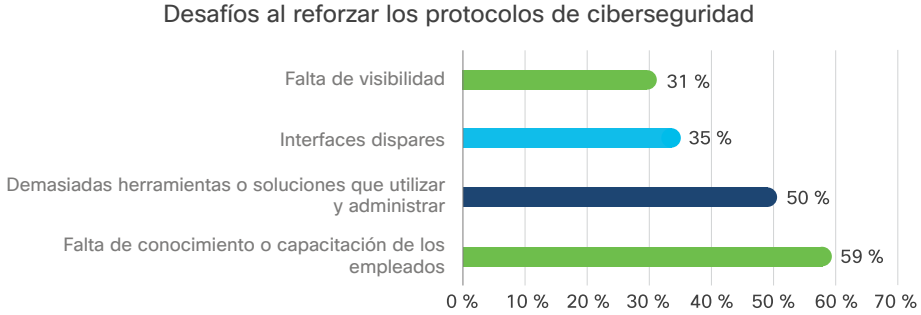
Magnitud de los cambios permanentes en las políticas de ciberseguridad según la región

VARIACIONES DEL TAMAÑO DE LA ORGANIZACIÓN (PEQUEÑAS, MEDIANAS Y GRANDES):

- Como era de esperarse, en las empresas más grandes (52 %), ***más del 30 %*** de los cambios en las políticas son permanentes, en comparación con las organizaciones pequeñas y medianas.
- Por otro lado, en las empresas pequeñas (55 %) y medianas (54 %), son permanentes el ***30 % o menos*** de las nuevas políticas de ciberseguridad.

Educación y cultura de seguridad: una necesidad

Dicho esto, se necesita más educación y mejor seguridad, que sean simples, fáciles de usar, y que funcionen en conjunto. El 59 % de las organizaciones de todo el mundo afirmó que la falta de conocimiento y educación de los empleados es el principal desafío al reforzar los protocolos de ciberseguridad para el trabajo remoto. El siguiente es que son demasiadas herramientas o soluciones que utilizar y administrar (50 %). Se observaron tendencias similares en APJC, América y Europa.



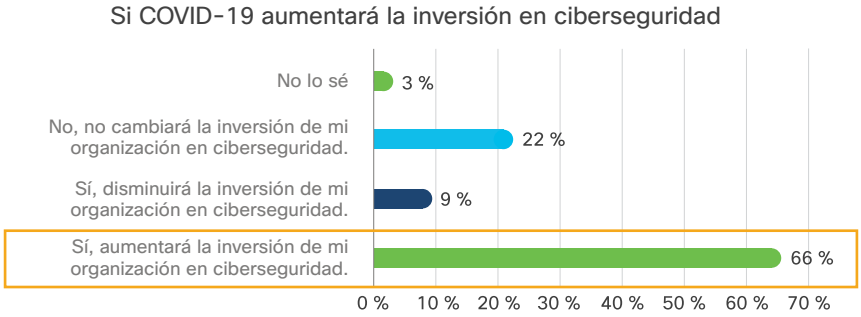
Global	APJC	AMER	Europa
Falta de conocimiento o capacitación de los empleados (59 %)	Falta de conocimiento o capacitación de los empleados (61 %)	Falta de conocimiento o capacitación de los empleados (58 %)	Falta de conocimiento o capacitación de los empleados (54 %)
Demasiadas herramientas o soluciones que utilizar y administrar (50 %)	Demasiadas herramientas o soluciones que utilizar y administrar (53 %)	Demasiadas herramientas o soluciones que utilizar y administrar (49 %)	Demasiadas herramientas o soluciones que utilizar y administrar (43 %)
Interfaces dispares (35 %)	Interfaces dispares (40 %)	Interfaces dispares (33 %)	Interfaces dispares (22 %)

Los 3 principales desafíos al reforzar los protocolos de ciberseguridad en todas las regiones

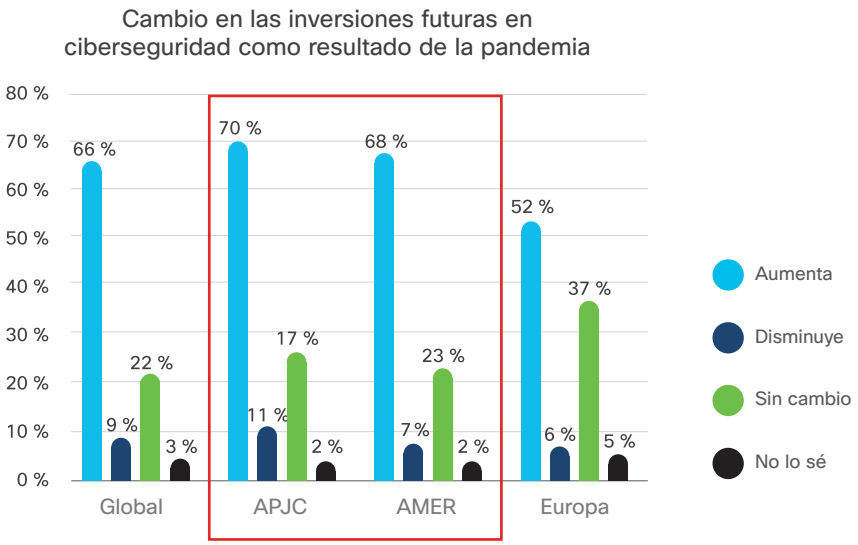
Los resultados muestran que hay una oportunidad para que el sector de seguridad cambie de manera fundamental para adaptarse a este momento y aumente su flexibilidad para admitir una fuerza laboral distribuida, donde la seguridad sea un facilitador en lugar de un obstáculo para la colaboración. Exploramos más este punto a continuación.

Aumentan las inversiones en ciberseguridad

Con estos cambios y mejoras en curso, la mayoría de las organizaciones de todo el mundo (66 %) indicó que probablemente aumentarán sus inversiones en ciberseguridad debido a la situación impuesta por la COVID-19.

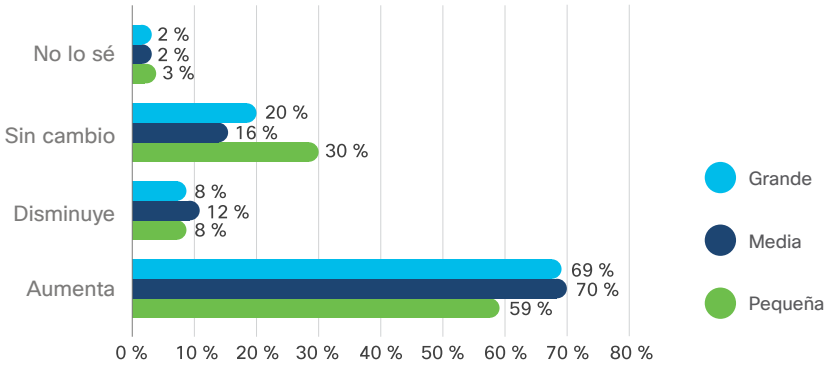


Más encuestados en APJC (70 %) y América (68 %) indicaron que aumentarán sus inversiones futuras en ciberseguridad, en comparación con el promedio global del 66 %.



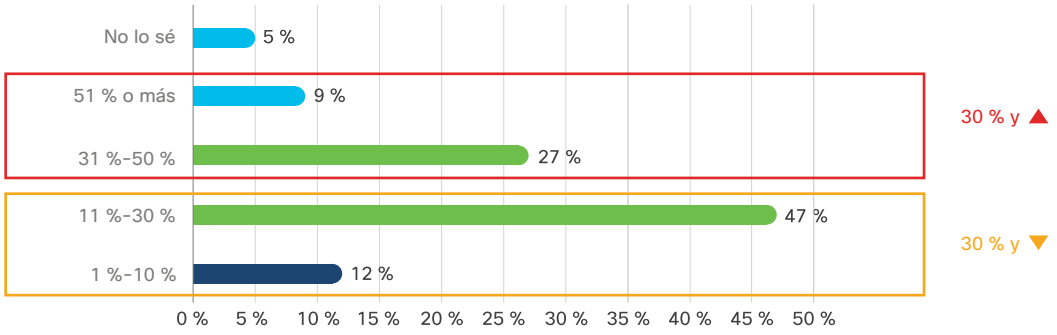
En desarrollos más positivos, las organizaciones de todos los tamaños buscan aumentar sus inversiones en ciberseguridad después de la pandemia. Curiosamente, las empresas medianas están ligeramente por delante de las grandes organizaciones, con un 70 % en busca de aumentar el gasto. Las pequeñas organizaciones tampoco se quedan atrás, con un 59 % que planea hacer lo mismo.

Cambio en las inversiones futuras en ciberseguridad según el tamaño de la organización



Si bien las organizaciones de todos los sectores, regiones y mercados están de acuerdo en la necesidad de aumentar el gasto en ciberseguridad, la proporcionalidad de dichas inversiones varía. En su mayor parte, el 59 % de quienes planean aumentar las inversiones en ciberseguridad indicaron un aumento previsto de entre ***el 1 % y el 30 %***. Esta tendencia se refleja en APJC (58 %), América (56 %) y Europa (65 %).

Proporción de aumento de las inversiones en ciberseguridad

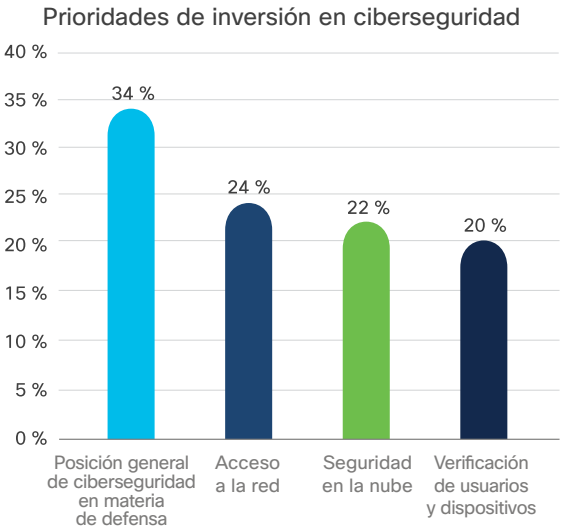


Proporción de mayores inversiones	Global	APJC	AMER	Europa
30 % o menos	59 %	58 %	56 %	65 %
Más del 30 %	36 %	39 %	39 %	23 %

Las organizaciones de todo el mundo están reconsiderando su estrategia general de seguridad

Cuando se les pidió que clasifiquen las inversiones en ciberseguridad según su importancia al prepararse para el mundo posterior a la pandemia de COVID-19, la postura general de defensa en materia de ciberseguridad, incluida la protección contra amenazas, las evaluaciones de riesgos, las auditorías, el cumplimiento y la privacidad, etc., es la prioridad de inversión más alta (el 34 % la clasificó en primer lugar). También es la opción más elegida para 16 de los 21 mercados encuestados. Esto indica que el entorno de trabajo remoto ha creado desafíos estratégicos que las empresas deben abordar al repensar las mejores maneras de hacer posible el entorno de trabajo flexible e híbrido, que llegó para quedarse.

Otras de las inversiones prioritarias que indicaron las organizaciones incluyen el acceso a la red (24 % en primer lugar), seguridad en la nube (22 % en primer lugar) y verificación de usuarios y dispositivos (20 % en primer lugar).



Prioridades de inversión en ciberseguridad en primer lugar

VARIACIONES REGIONALES

APJC	AMER	Europa
Postura general de defensa en materia de ciberseguridad (35 %)	Postura general de defensa en materia de ciberseguridad (31 %)	Postura general de defensa en materia de ciberseguridad (33 %)
Seguridad en la nube (23 %)	Seguridad en la nube (25 %)	Acceso a la red (29 %)
Acceso a la red (23 %)	Acceso a la red (22 %)	Verificación de usuarios y dispositivos (21 %)

RESULTADOS CLAVE Y RECOMENDACIONES

RESULTADOS CLAVE Y RECOMENDACIONES

N.º 1 El futuro del trabajo es dinámico: la ciberseguridad debe satisfacer las necesidades de una fuerza laboral distribuida.

El mundo ahora ve que es posible que los empleados se mantengan conectados y productivos trabajando fuera de la oficina durante períodos prolongados. Es probable que muchas empresas avancen hacia un entorno de trabajo híbrido, que admita tanto empleados remotos como en la oficina. Esto ofrecerá al empleador y a los empleados más opciones y mayor flexibilidad desde el punto de vista de la empresa y el capital humano, además de aportar más diversidad a la fuerza laboral. El cambio brusco también generó una serie de desafíos de ciberseguridad: mantener la empresa en funcionamiento en un entorno muy distinto o la necesidad de proteger el acceso a una escala mayor que antes.

Los empleados conectan los dispositivos de la oficina a la red Wi-Fi de su hogar o a redes externas, o utilizan dispositivos personales para conectarse con las aplicaciones corporativas en la nube. Esto ejerce una presión repentina sobre los equipos de TI y de seguridad, que ahora deben encargarse de brindar soporte rápidamente a una cantidad sin precedentes de trabajadores fuera del sitio y sus dispositivos, sin comprometer la seguridad. Las políticas y los controles que una vez residieron en la sede central ahora deben seguir al trabajador adonde sea y cuando sea que requiera acceso. Además, la oportunidad del trabajo remoto tiene un lado oscuro: los agentes maliciosos modernos han lanzado más ataques de suplantación de identidad (phishing) para engañar a los usuarios y robarles información, comprometer con malware los sistemas de la fuerza laboral que recién se inicia en la modalidad remota o aprovechar las brechas en la evolución de la postura de ciberseguridad de una empresa.

Las empresas deben crear un entorno de trabajo híbrido flexible y seguro, en el que los empleados se puedan conectar y desconectar de la red con niveles similares de protección. A medida que los líderes empresariales y de TI hacen cambios significativos en las prioridades tecnológicas y empresariales, la ciberseguridad debe ser el puente que permita que las organizaciones alcancen su máximo potencial.

N.º 2 El éxito de una fuerza laboral híbrida flexible depende de la preparación, la colaboración y el empoderamiento.

Una de las cuestiones clave que surgieron con el paso brusco al trabajo remoto en los últimos ocho meses es cómo las organizaciones lograron hacer la transición. Las empresas que hicieron inversiones graduales y continuas en tecnología antes de la pandemia, como soluciones de seguridad en la nube y marcos de confianza cero, han sido las mejor preparadas para permitir el trabajo remoto. Asimismo, la mejora de las medidas de ciberseguridad que respaldan dichos acuerdos ha colocado a las organizaciones en una mejor posición para enfrentar el posible aumento en la cantidad y variedad de los ataques de ciberseguridad.

Sin embargo, con el fin de obtener todos los beneficios de un lugar de trabajo flexible e híbrido, dichas inversiones no pueden hacerse en el vacío. Con el pasaje a una fuerza laboral distribuida, los equipos de red y de seguridad deben proporcionar un acceso seguro e impecable a las aplicaciones y los servicios, en cualquier lugar y en cualquier momento. La seguridad, las redes y la colaboración ya no pueden presentarse en silos. Deben funcionar de la mano. Junto con estas funciones, los líderes deben establecer protocolos de control adicionales y políticas de ciberseguridad mejoradas. Esto también debe complementarse con un programa sólido de educación de los empleados, dado que la inversión en una cultura de seguridad saludable es absolutamente fundamental.

N.º 3 Una ciberseguridad más simple y eficaz es fundamental para desarrollar la resiliencia empresarial.

La experiencia del trabajo remoto prolongado ha puesto en evidencia el valor de la ciberseguridad en las agendas corporativas, con posibles cambios a largo plazo en las políticas de ciberseguridad corporativa. Además, muchos indicaron que tienen la intención de aumentar el gasto en ciberseguridad en el futuro.

Son muchas las prioridades que compiten por la atención de los líderes de TI y la seguridad no puede ser una idea de último momento, sino que debe ser la base del éxito de cualquier iniciativa de digitalización. Esto garantizará la seguridad, la escalabilidad y la adaptabilidad de estas iniciativas. Para reducir la probabilidad y el impacto de una violación a la ciberseguridad, las organizaciones también deben buscar formas de reducir la complejidad de sus medidas de ciberseguridad. Adoptar un enfoque simplificado respecto de una seguridad más eficaz garantiza que sea un facilitador de los negocios, no un obstáculo para lo que se necesita ahora y para lo que se viene.

Recomendaciones:

Para que las empresas permitan que las personas trabajen de forma segura desde cualquier lugar, en cualquier momento y con cualquier dispositivo, la ciberseguridad debe ser la base de toda inversión en TI. Esto requiere un enfoque en materia de plataformas que ofrezca seguridad sumamente eficaz desde la red hasta el terminal y la nube. No es suficiente contar con productos individuales, por buenos que sean. Cuando la seguridad debe ofrecer menos complejidad, las soluciones deben funcionar juntas y ofrecer facilidad de uso.

Para habilitar de manera segura una fuerza laboral distribuida y garantizar la flexibilidad para adaptarse a lo que ofrece el futuro del trabajo, las organizaciones deben asegurarse de que se cumplan las siguientes condiciones:

- Verificar la identidad de los usuarios para establecer confianza: ¿es usted quien dice ser?
- Permitir trabajar en cualquier tipo de dispositivo y con cualquier tipo de conexión, de forma segura
- Dar acceso a las aplicaciones y los datos de la empresa que necesitan los trabajadores
- Proteger a los usuarios de las amenazas una vez que están en la red

Futuro del trabajo: 10 conclusiones

1. Adopte una estrategia de confianza cero para verificar la identidad de todos los usuarios antes de otorgar acceso a las aplicaciones aprobadas por la empresa: proteja la fuerza laboral, la carga de trabajo y el lugar de trabajo.
2. La autenticación de varios factores (MFA) es, naturalmente, el primer paso en la protección de una fuerza laboral distribuida; le permite verificar las identidades de los empleados que intentan acceder a los recursos corporativos.
3. Implemente una VPN que proporcione un túnel seguro entre los usuarios y las aplicaciones para que los trabajadores puedan mantenerse productivos y conectados cuando están de viaje o trabajan desde la casa. Esto ayuda a garantizar que solo ingresen usuarios aprobados, ya que proporciona el nivel adecuado de seguridad sin comprometer la experiencia del usuario.
4. Use DNS. La mayoría de las violaciones de seguridad apuntan a los usuarios de terminales, lo que requiere una primera línea de defensa en la capa de DNS. Esta primera capa, que es decisiva, bloquea los dominios asociados al comportamiento malicioso antes de que ingresen a la red o de que contengan malware si ya entraron.
5. Proteja el correo electrónico de Office 365 de las amenazas avanzadas. Dado que el correo electrónico es el principal vector de ataque, se necesita protección contra las amenazas de correo electrónico como la suplantación de identidad (phishing), el ransomware, el compromiso del correo electrónico empresarial y otros mediante una solución de seguridad integrada y nativa de la nube para Microsoft 365 que detenga las amenazas a Office 365 tanto de los remitentes internos como externos.
6. Mantenga la última línea de defensa con soluciones seguras para terminales. La seguridad de los terminales no solo evita los ataques cibernéticos, sino que también detecta, contiene y corrige rápidamente los archivos maliciosos si evaden las defensas y se infiltran en los terminales, antes de que se produzcan daños.
7. Acelere la adopción estratégica de soluciones de seguridad basadas en la nube para proteger su fuerza laboral mediante una conexión impecable con las aplicaciones en cualquier entorno y desde cualquier ubicación. El perímetro de servicio de acceso seguro (SASE) es una arquitectura de red que combina capacidades de SD-WAN con funciones de seguridad nativas de la nube como gateways web seguros, agentes de seguridad de acceso a la nube y firewalls, todo desde la nube.
8. Obtenga mayores beneficios de los productos existentes mediante un enfoque de plataforma. Esto permite ver todas las soluciones de seguridad en un tablero unificado, a la vez que se integra con soluciones de seguridad de terceros.
9. Automatice los flujos de trabajo del Centro de operaciones de seguridad (SOC), como la investigación, la búsqueda y la corrección de amenazas para fortalecer la eficiencia y la precisión, sin aumentar los costos operativos. De esta manera, los equipos de seguridad pueden responder mejor a las cambiantes necesidades empresariales y de tecnología, y mantener la anticipación frente al panorama de amenazas en constante cambio.
10. Recuerde: las personas pueden ser el eslabón más fuerte en cualquier tipo de defensa. Fomente un mayor conocimiento de la ciberseguridad y el empoderamiento entre los empleados. Las organizaciones también deben buscar que los empleados tengan una mayor noción de la importancia de adoptar prácticas centradas en la seguridad, como aprender a identificar ataques de suplantación de identidad (phishing), practicar una buena política de contraseñas y mantener el software actualizado. La capacitación en ciberseguridad no puede ser un curso anual exigido por motivos de cumplimiento, que a la mayoría de los empleados le disgusta. Debe ser parte de la cultura.

Cisco SecureX ™ es una experiencia de plataforma nativa de la nube que conecta el portafolio de seguridad y redes de Cisco con la infraestructura existente. Es integrada y abierta para que sea más simple de utilizar, está unificada en una sola ubicación para mejorar la visibilidad y maximiza la eficiencia operativa con flujos de trabajo automatizados.

PUNTOS DESTACADOS DE AMÉRICA

PUNTOS DESTACADOS DE AMÉRICA

Resumen regional

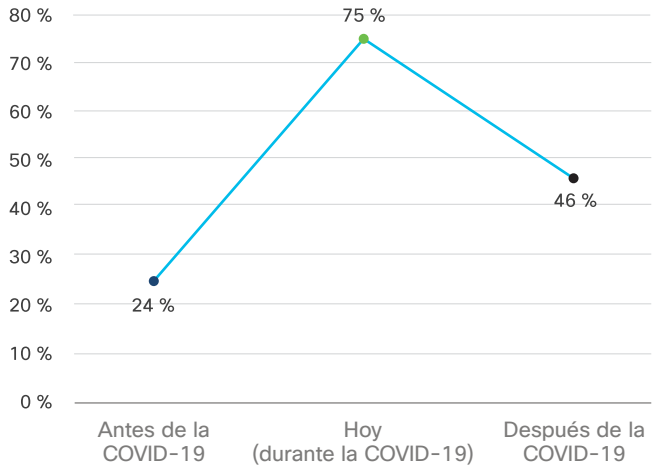
El estudio encuestó a más de 600 organizaciones de cuatro países de América: Brasil, Canadá, México y Estados Unidos. Antes de que la pandemia presentara la oportunidad de hacer un gran experimento global sobre los costos y beneficios de una fuerza laboral totalmente remota, muchas personas del mercado de América ya trabajaban fuera de las oficinas tradicionales. Incluso entonces, el pasaje de la noche a la mañana a una fuerza laboral remota aún planteaba una serie de desafíos de ciberseguridad para las empresas. Solo el 39 % de las organizaciones de América indicaron estar ***muy preparadas*** para la transición repentina a un entorno de trabajo remoto, cifra un poco más baja que el promedio global del 40 % y el promedio europeo del 45 %. El 55 % de las organizaciones del mercado de América indicó estar ***algo preparada*** y el 6 % se consideró ***sin preparación***. El mercado de América también presentó más organizaciones que experimentaron un salto del ***25 % o más*** en la cantidad de amenazas o alertas cibernéticas desde el comienzo de la COVID-19 (64 %) en comparación con el promedio global del 61 %.

De todas las regiones encuestadas, el mercado de América presentó el mayor porcentaje de organizaciones (88 %) que afirmó que la ciberseguridad ahora es ***sumamente importante o más importante que antes de la pandemia de COVID-19***, en comparación con el 85 % en APJC y el 81 % en Europa. Como resultado, casi todas las organizaciones encuestadas indicaron que realizaron cambios en sus políticas de ciberseguridad para respaldar el trabajo remoto (97 %); casi 7 de cada 10 (68 %) organizaciones proyectan un aumento en las inversiones futuras en ciberseguridad debido a la pandemia de COVID-19.

Hallazgos clave

Las organizaciones del mercado de América están transitando hacia un futuro de trabajo híbrido, pero pueden mejorar su preparación para la ciberseguridad

Porcentaje de organizaciones con más del 50 % de trabajadores remotos en el mercado de América



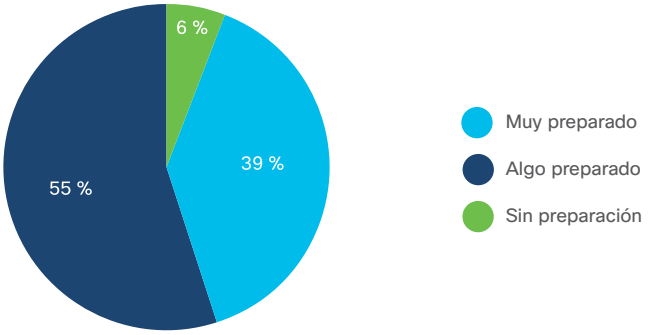
	Global	AMER
Antes de la COVID-19	19 %	24 %
Hoy (durante la COVID-19)	62 %	75 %
Después de la COVID-19	37 %	46 %

El mercado de América no es ajeno al trabajo remoto: ya antes de la pandemia había marcado el récord de nómadas digitales más alto del mundo. El 24 % de las organizaciones ya tenía ***más de la mitad*** de su fuerza laboral trabajando de manera remota antes de la pandemia. Esta cifra se triplicó (75 %) durante el brote y se prevé que baje al 46 % después de la pandemia de COVID-19.

- México presentó la mayor proporción de organizaciones (77 %) en América, con ***más de la mitad*** de su fuerza laboral trabajando de manera remota durante la pandemia. A partir de esto, un sorprendente 40 % de las organizaciones mexicanas espera que ***más de la mitad*** de sus empleados sigan siendo remotos, incluso en el mundo posterior a la pandemia.
- Las organizaciones en los Estados Unidos (50 %) y Brasil (53 %) están superando la tendencia del trabajo remoto después de la pandemia; es mayor la proporción de organizaciones que esperan que ***más de la mitad*** de su fuerza laboral trabaje de manera remota, en comparación con el promedio global del 37 %.

La mayoría de las organizaciones de la región estaban ***algo preparadas*** (55 %) para la transición al trabajo remoto a gran escala. De manera similar a APJC, solo el 39 % de las organizaciones de América estaba ***muy preparado*** para el cambio repentino, mientras que otro 6 % ***no estaba preparado***.

Nivel de preparación para la transición al trabajo remoto entre las organizaciones en el mercado de América



Nivel de preparación para la transición al trabajo remoto	Global	APJC	AMER	Europa
Muy preparado	40 %	39 %	39 %	45 %
Algo preparado	53 %	54 %	55 %	50 %
Sin preparación	6 %	7 %	6 %	6 %

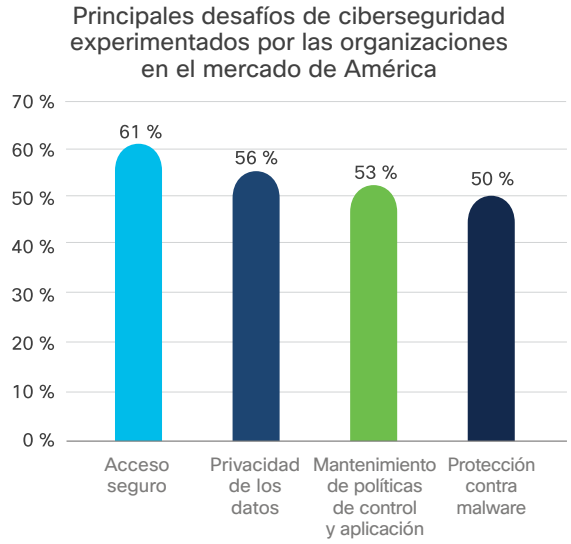
- Estados Unidos presentó la mayor proporción de organizaciones que estaban ***muy preparadas*** (46 %) para la transición repentina al trabajo remoto en la región (entre un 6 % y un 7 % más que el promedio global y regional).

Abordar las amenazas y los desafíos de ciberseguridad en América

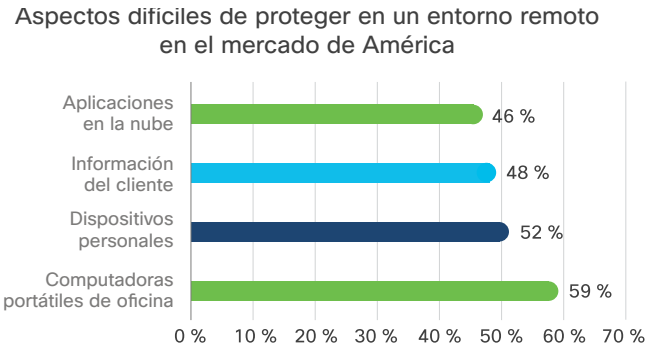
A nivel regional, el 64 % de los encuestados en América experimentó un salto del ***25 % o más*** en la cantidad de amenazas o alertas cibernéticas desde el comienzo de la pandemia de COVID-19, cifra levemente superior al promedio global del 61 %.

- Este número varía en las diferentes áreas de la región; la mayor proporción de encuestados que experimentó un salto del ***25 % o más*** en amenazas o alertas cibernéticas es de Brasil (82 %).
- El 54 % de los encuestados de los Estados Unidos y el 53 % de los encuestados de Canadá experimentaron un salto del 25 % o más en la cantidad de amenazas o alertas cibernéticas, cifra menor que los promedios regionales y globales.
- El 10 % de los encuestados de los Estados Unidos no sabía si las amenazas o alertas cibernéticas habían aumentado o disminuido. Esta cifra es más alta que el promedio global del 8 %, y también la más alta dentro de América.

Al igual que con las empresas de todo el mundo, las organizaciones de América descubrieron que la transición al trabajo con distanciamiento social se ve obstaculizada por los desafíos de ciberseguridad. El 61 % de las organizaciones de América afirmó que el **acceso seguro es el principal desafío de ciberseguridad** que enfrentan la mayoría de las organizaciones cuando se trata de contar con trabajadores remotos. Otras inquietudes planteadas por las organizaciones de América incluyen la privacidad de los datos (56 %), que tiene implicaciones para la postura general en materia de seguridad, el mantenimiento del control y la aplicación de políticas (53 %), y la protección contra malware (50 %).



Cuando los trabajadores comenzaron a quedarse en sus casas, muchos usaban dispositivos no tan seguros como los de la oficina. Con las consecuencias de las redes mal protegidas al trabajar desde el hogar, muchas empresas consideran que las computadoras portátiles o de escritorio de la oficina (59 %) y los dispositivos personales (52 %) son difíciles de proteger en un entorno remoto; a esto le sigue la información de los clientes (48 %).



- La misma proporción de encuestados de Brasil indicó que la información de los clientes es un aspecto difícil de proteger; las computadoras portátiles o de escritorio de la empresa representan el 58 %, más que los dispositivos personales (53 %).

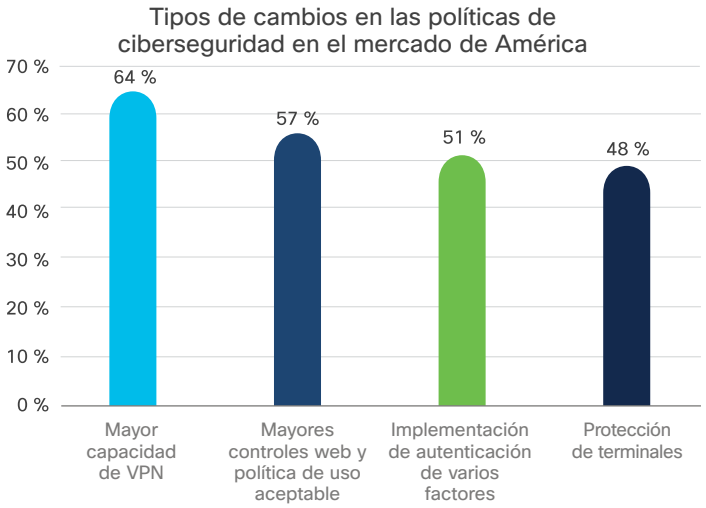
Priorizar la ciberseguridad para el presente y para lo que se viene

Las medidas de ciberseguridad son claramente la prioridad para las organizaciones de América: el 57 % de los adoptantes las clasifican como la prioridad número uno entre todas las soluciones de tecnología adoptadas para permitir el trabajo remoto; esta cifra es más alta que el promedio global del 52 %, que las clasificó en primer lugar, Estados Unidos a la cabeza con el 62 % (clasificadas en primer lugar).

Los encuestados de México (57 %) y Brasil (58 %) presentaron una mayor proporción de organizaciones que indicaron que la ciberseguridad es ***sumamente importante*** en comparación con Estados Unidos (43 %) y Canadá (42 %), y más que el promedio de América del 50 %.

Importancia de la ciberseguridad	EE. UU.	Canadá	México	Brasil
Sumamente importante	43 %	42 %	57 %	58 %
Más importante que antes	39 %	42 %	34 %	37 %
Algo importante	17 %	15 %	8 %	4 %
No importante	1 %	1 %	1 %	0 %

Importancia de la ciberseguridad para la organización según los países en América



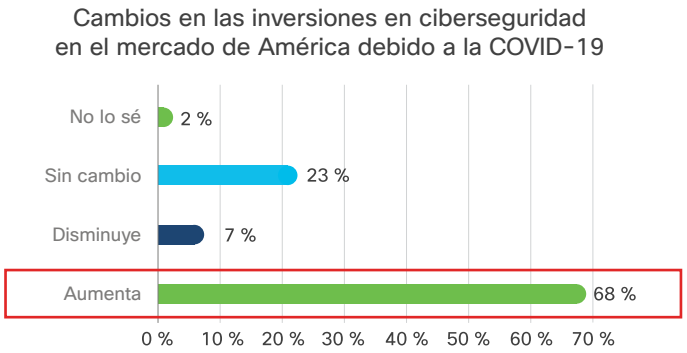
El 97 % de las organizaciones de América hicieron cambios en las políticas de ciberseguridad para respaldar la fuerza laboral remota; esto responde a las tendencias globales con un aumento cada vez más pronunciado en ciertas áreas.

Para reforzar las defensas de los empleados remotos, el principal cambio relacionado con las políticas fue el **aumento de la capacidad de VPN**, que implementaron dos tercios de las organizaciones de América (64 %), cifra superior al promedio global (59 %) y de APJC (56 %), y similar al de Europa (64 %). A esto le sigue el **aumento de los controles web y una política de uso aceptable** del 57 %, también ligeramente superior a la cifra global (55 %), y la implementación de la **autenticación de varios factores** (51 %), un 2 % inferior al porcentaje global.

- En Brasil, 7 de cada 10 organizaciones aumentaron su capacidad de VPN (71 %). Esto lo convierte en el país con la mayor proporción de organizaciones que optaron por aumentar la capacidad de VPN como cambio principal de política en materia de ciberseguridad, en la región y en el mundo.
- Si bien América destacó el aumento de la capacidad de VPN como el principal cambio en la política de ciberseguridad durante la pandemia, el 67 % de las organizaciones de México también realizó cambios en la protección de los terminales.

Aumentan las inversiones en ciberseguridad

Como resultado de los desafíos en torno a la pandemia, se espera que los presupuestos de ciberseguridad para más de dos tercios (68 %) de las organizaciones de América aumenten. Sin embargo, casi una cuarta parte indicó que las inversiones futuras en ciberseguridad se mantendrán igual (23 %), en sintonía con el promedio global (22 %).



Cambios en las inversiones en ciberseguridad debido a la pandemia de COVID-19	Global	APJC	AMER	Europa
Aumente	66 %	70 %	68 %	52 %
Disminuya	9 %	11 %	7 %	6 %
Sin cambio	22 %	17 %	23 %	37 %
No lo sé	3 %	2 %	2 %	5 %

- Brasil presentó la mayor proporción de encuestados que indican que la situación de la pandemia de COVID-19 dará lugar a un aumento en sus inversiones futuras en ciberseguridad (78 %), en comparación con el promedio global del 66 % y el promedio regional del 68 %. De hecho, el 48 % de quienes indicaron un aumento en Brasil prevén un incremento de las inversiones de ***más del 30 %***, la cifra más alta de la región de América.

Un enfoque en la postura general de defensa en materia de ciberseguridad obtiene la mayor parte (el 31 % la clasificó en primer lugar) de la inversión de la región, como la mayor prioridad de inversión en América. Otras inversiones prioritarias que indicaron las organizaciones de América son la seguridad en la nube (25 % en primer lugar) y el acceso a la red (22 % en primer lugar).

PAÍSES EN PROFUNDIDAD: AMÉRICA

Brasil

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
La importancia de la ciberseguridad en un futuro laboral híbrido			
Porcentaje de organizaciones con ***más de la mitad*** de la fuerza laboral trabajando en modalidad remota	· Antes de la COVID-19: 25 % · Durante la COVID-19: 76 % · Después de la COVID-19: 53 %	· Antes de la COVID-19: 24 % · Durante la COVID-19: 75 % · Después de la COVID-19: 46 %	· Antes de la COVID-19: 19 % · Durante la COVID-19: 62 % · Después de la COVID-19: 37 %
Importancia de la ciberseguridad para las organizaciones	· Sumamente importante: 58 % · Más importante que antes: 37 % · Algo importante: 4 %	· Sumamente importante: 50 % · Más importante que antes: 38 % · Algo importante: 11 %	· Sumamente importante: 44 % · Más importante que antes: 41 % · Algo importante: 15 %
Un repunte resiliente: abordar las amenazas y los desafíos en materia de ciberseguridad			
Nivel de aumento de amenazas y alertas cibernéticas	· Aumento del 25 % o más: 82 % · No sabe: 2 %	· Aumento del 25 % o más: 64 % · No sabe: 5 %	· Aumento del 25 % o más: 61 % · No sabe: 8 %
Los 3 principales desafíos de ciberseguridad	· Privacidad de los datos: 68 % · Acceso seguro: 63 % · Protección contra malware: 61 %	· Acceso seguro: 61 % · Privacidad de los datos: 56 % · Mantenimiento de políticas de control y aplicación: 53 %	· Acceso seguro: 62 % · Privacidad de los datos: 55 % · Mantenimiento de políticas de control y aplicación: 50 %
Aspecto difícil de proteger en un entorno remoto	· Información de los clientes Y computadoras portátiles o de escritorio de la oficina: 58 % · Dispositivos personales: 53 % · Aplicaciones en la nube: 51 %	· Computadoras portátiles o de escritorio de la oficina: 59 % · Dispositivos personales: 52 % · Información de los clientes: 48 % · Aplicaciones en la nube: 46 %	· Computadoras portátiles o de escritorio de la oficina: 56 % · Dispositivos personales: 54 % · Información de los clientes Y aplicaciones en la nube: 46 %
Preparación para la transición a un entorno de trabajo remoto al comienzo de la pandemia de COVID-19	· Muy preparado: 39 % · Algo preparado: 55 % · Sin preparación: 6 %	· Muy preparado: 39 % · Algo preparado: 55 % · Sin preparación: 6 %	· Muy preparado: 40 % · Algo preparado: 53 % · Sin preparación: 6 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Priorizar la ciberseguridad para el presente y para lo que se viene			
Las 3 principales soluciones de TI adoptadas para permitir el trabajo remoto	· Herramientas de colaboración: 77 % · Medidas de ciberseguridad: 73 % · Uso compartido de documentos en la nube: 71 %	· Herramientas de colaboración: 73 % · Medidas de ciberseguridad: 68 % · Uso compartido de documentos en la nube: 64 %	· Herramientas de colaboración: 73 % · Medidas de ciberseguridad: 68 % · Uso compartido de documentos en la nube: 63 %
Soluciones de TI adoptadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Medidas de ciberseguridad: 51 % · Herramientas de colaboración: 31 % · Servicios profesionales: 29 %	· Medidas de ciberseguridad: 57 % · Herramientas de colaboración: 36 % · Protección de datos distribuidos: 23 %	· Medidas de ciberseguridad: 52 % · Herramientas de colaboración: 41 % · Servicios profesionales: 27 %
Los 3 principales cambios en las políticas de ciberseguridad para permitir el trabajo remoto	· Mayor capacidad de VPN: 71 % · Mayores controles web y política de uso aceptable: 67 % · Implementación de autenticación de varios factores: 63 %	· Mayor capacidad de VPN: 64 % · Mayores controles web y política de uso aceptable: 57 % · Implementación de autenticación de varios factores: 51 %	· Mayor capacidad de VPN: 59 % · Mayores controles web y política de uso aceptable: 55 % · Implementación de autenticación de varios factores: 53 %
Proporción de cambios permanentes en las políticas de ciberseguridad	· 30 % o menos: 45 % · Más del 30 %: 55 %	· 30 % o menos: 44 % · Más del 30 %: 54 %	· 30 % o menos: 50 % · Más del 30 %: 45 %
Los 3 desafíos principales en la aplicación de los protocolos de ciberseguridad	· Demasiadas herramientas o soluciones que utilizar y administrar: 64 % · Falta de conocimiento o capacitación de los empleados: 55 % · Interfaces dispares: 33 %	· Falta de conocimiento o capacitación de los empleados: 58 % · Demasiadas herramientas o soluciones que utilizar y administrar: 49 % · Interfaces dispares: 33 %	· Falta de conocimiento o capacitación de los empleados: 59 % · Demasiadas herramientas o soluciones que utilizar y administrar: 50 % · Interfaces dispares: 35 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Inversiones en ciberseguridad en aumento			
Cambio en la inversión futura de la organización en ciberseguridad debido a la pandemia de COVID-19	· Aumento: 78 % · Disminución: 9 % · Sin cambios: 13 %	· Aumento: 68 % · Disminución: 7 % · Sin cambios: 23 %	· Aumento: 66 % · Disminución: 9 % · Sin cambios: 22 %
Proporción de aumento de la inversión futura en ciberseguridad	· 30 % o menos: 52 % · Más del 30 %: 48 %	· 30 % o menos: 56 % · Más del 30 %: 39 %	· 30 % o menos: 59 % · Más del 30 %: 36 %
Inversiones en ciberseguridad clasificadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Postura general de defensa en materia de ciberseguridad: 34 % · Seguridad en la nube: 26 % · Verificación de usuarios y dispositivos: 23 % · Acceso a la red: 16 %	· Postura general de defensa en materia de ciberseguridad: 31 % · Seguridad en la nube: 25 % · Acceso a la red Y verificación de usuarios y dispositivos: 22 % (EN CONJUNTO)	· Postura general de defensa en materia de ciberseguridad: 34 % · Acceso a la red: 24 % · Seguridad en la nube: 22 % · Verificación de usuarios y dispositivos: 20 %

Canadá

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
La importancia de la ciberseguridad en un futuro del trabajo híbrido			
Porcentaje de organizaciones con ***más de la mitad*** de la fuerza laboral trabajando en modalidad remota	· Antes de la COVID-19: 20 % · Durante la COVID-19: 75 % · Después de la COVID-19: 42 %	· Antes de la COVID-19: 24 % · Durante la COVID-19: 75 % · Después de la COVID-19: 46 %	· Antes de la COVID-19: 19 % · Durante la COVID-19: 62 % · Después de la COVID-19: 37 %
Importancia de la ciberseguridad para las organizaciones	· Sumamente importante: 42 % · Más importante que antes: 42 % · Algo importante: 15 %	· Sumamente importante: 50 % · Más importante que antes: 38 % · Algo importante: 11 %	· Sumamente importante: 44 % · Más importante que antes: 41 % · Algo importante: 15 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Un repunte resiliente: abordar las amenazas y los desafíos en materia de ciberseguridad			
Nivel de aumento de amenazas y alertas cibernéticas	· Aumento del 25 % o más: 53 % · No sabe: 4 %	· Aumento del 25 % o más: 64 % · No sabe: 5 %	· Aumento del 25 % o más: 61 % · No sabe: 8 %
Los 3 principales desafíos de ciberseguridad	· Acceso seguro: 61 % · Privacidad de los datos: 54 % · Mantenimiento de políticas de control y aplicación y protección contra malware: 52 %	· Acceso seguro: 61 % · Privacidad de los datos: 56 % · Mantenimiento de políticas de control y aplicación: 53 %	· Acceso seguro: 62 % · Privacidad de los datos: 55 % · Mantenimiento de políticas de control y aplicación: 50 %
Aspecto difícil de proteger en un entorno remoto	· Computadoras portátiles o de escritorio de la oficina: 56 % · Información de los clientes: 50 % · Dispositivos personales: 47 % · Aplicaciones en la nube: 45 %	· Computadoras portátiles o de escritorio de la oficina: 59 % · Dispositivos personales: 52 % · Información de los clientes: 48 % · Aplicaciones en la nube: 46 %	· Computadoras portátiles o de escritorio de la oficina: 56 % · Dispositivos personales: 54 % · Información de los clientes Y aplicaciones en la nube: 46 % (EN CONJUNTO)
Preparación para la transición a un entorno de trabajo remoto al comienzo de la pandemia de COVID-19	· Muy preparado: 39 % · Algo preparado: 56 % · Sin preparación: 6 %	· Muy preparado: 39 % · Algo preparado: 55 % · Sin preparación: 6 %	· Muy preparado: 40 % · Algo preparado: 53 % · Sin preparación: 6 %
Priorizar la ciberseguridad para el presente y para lo que se viene			
Las 3 principales soluciones de TI adoptadas para permitir el trabajo remoto	· Uso compartido de documentos en la nube: 73 % · Medidas de ciberseguridad: 71 % · Herramientas de colaboración: 68 %	· Herramientas de colaboración: 73 % · Medidas de ciberseguridad: 68 % · Uso compartido de documentos en la nube: 64 %	· Herramientas de colaboración: 73 % · Medidas de ciberseguridad: 68 % · Uso compartido de documentos en la nube: 63 %
Soluciones de TI adoptadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Medidas de ciberseguridad: 59 % · Uso compartido de documentos en la nube: 33 % · Herramientas de colaboración: 27 %	· Medidas de ciberseguridad: 57 % · Herramientas de colaboración: 36 % · Protección de datos distribuidos: 23 %	· Medidas de ciberseguridad: 52 % · Herramientas de colaboración: 41 % · Servicios profesionales: 27 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Los 3 principales cambios en las políticas de ciberseguridad para permitir el trabajo remoto	· Mayor capacidad de VPN: 67 % · Mayores controles web y política de uso aceptable: 58 % · Protección de terminales: 53 %	· Mayor capacidad de VPN: 64 % · Mayores controles web y política de uso aceptable: 57 % · Implementación de autenticación de varios factores: 51 %	· Mayor capacidad de VPN: 59 % · Mayores controles web y política de uso aceptable: 55 % · Implementación de autenticación de varios factores: 53 %
Proporción de cambios permanentes en las políticas de ciberseguridad	· 30 % o menos: 48 % · Más del 30 %: 50 %	· 30 % o menos: 44 % · Más del 30 %: 54 %	· 30 % o menos: 50 % · Más del 30 %: 45 %
Los 3 desafíos principales en la aplicación de los protocolos de ciberseguridad	· Falta de conocimiento o capacitación de los empleados: 58 % · Demasiadas herramientas o soluciones que utilizar y administrar: 49 % · Falta de visibilidad: 35 %	· Falta de conocimiento o capacitación de los empleados: 58 % · Demasiadas herramientas o soluciones que utilizar y administrar: 49 % · Interfaces dispares: 33 %	· Falta de conocimiento o capacitación de los empleados: 59 % · Demasiadas herramientas o soluciones que utilizar y administrar: 50 % · Interfaces dispares: 35 %
Inversiones en ciberseguridad en aumento			
Cambio en la inversión futura de la organización en ciberseguridad debido a la pandemia de COVID-19	· Aumento: 74 % · Disminución: 5 % · Sin cambios: 19 %	· Aumento: 68 % · Disminución: 7 % · Sin cambios: 23 %	· Aumento: 66 % · Disminución: 9 % · Sin cambios: 22 %
Proporción de aumento de la inversión futura en ciberseguridad	· 30 % o menos: 62 % · Más del 30 %: 32 %	· 30 % o menos: 56 % · Más del 30 %: 39 %	· 30 % o menos: 59 % · Más del 30 %: 36 %
Inversiones en ciberseguridad clasificadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Postura general de defensa en materia de ciberseguridad: 30 % · Seguridad en la nube: 27 % · Acceso a la red: 22 % · Verificación de usuarios y dispositivos: 20 %	· Postura general de defensa en materia de ciberseguridad: 31 % · Seguridad en la nube: 25 % · Acceso a la red Y verificación de usuarios y dispositivos: 22 %	· Postura general de defensa en materia de ciberseguridad: 34 % · Acceso a la red: 24 % · Seguridad en la nube: 22 % · Verificación de usuarios y dispositivos: 20 %

México

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
La importancia de la ciberseguridad en un futuro laboral híbrido			
Porcentaje de organizaciones con ***más de la mitad*** de la fuerza laboral trabajando en modalidad remota	• Antes de la COVID-19: 19 % • Durante la COVID-19: 77 % • Después de la COVID-19: 40 %	• Antes de la COVID-19: 24 % • Durante la COVID-19: 75 % • Después de la COVID-19: 46 %	• Antes de la COVID-19: 19 % • Durante la COVID-19: 62 % • Después de la COVID-19: 37 %
Importancia de la ciberseguridad para las organizaciones	• Sumamente importante: 57 % • Más importante que antes: 34 % • Algo importante: 8 %	• Sumamente importante: 50 % • Más importante que antes: 38 % • Algo importante: 11 %	• Sumamente importante: 44 % • Más importante que antes: 41 % • Algo importante: 15 %
Un repunte resiliente: abordar las amenazas y los desafíos en materia de ciberseguridad			
Nivel de aumento de amenazas y alertas cibernéticas	• Aumento del 25 % o más: 65 % • No sabe: 6 %	• Aumento del 25 % o más: 64 % • No sabe: 5 %	• Aumento del 25 % o más: 61 % • No sabe: 8 %
Los 3 principales desafíos de ciberseguridad	• Acceso seguro: 62 % • Privacidad de los datos: 60 % • Mantenimiento de políticas de control y aplicación: 59 %	• Acceso seguro: 61 % • Privacidad de los datos: 56 % • Mantenimiento de políticas de control y aplicación: 53 %	• Acceso seguro: 62 % • Privacidad de los datos: 55 % • Mantenimiento de políticas de control y aplicación: 50 %
Aspecto difícil de proteger en un entorno remoto	• Computadoras portátiles o de escritorio de la oficina: 69 % • Dispositivos personales: 58 % • Aplicaciones en la nube: 50 % • Información de los clientes: 48 %	• Computadoras portátiles o de escritorio de la oficina: 59 % • Dispositivos personales: 52 % • Información de los clientes: 48 % • Aplicaciones en la nube: 46 %	• Computadoras portátiles o de escritorio de la oficina: 56 % • Dispositivos personales: 54 % • Información de los clientes Y aplicaciones en la nube: 46 % (EN CONJUNTO)
Preparación para la transición a un entorno de trabajo remoto al comienzo de la pandemia de COVID-19	• Muy preparado: 33 % • Algo preparado: 60 % • Sin preparación: 7 %	• Muy preparado: 39 % • Algo preparado: 55 % • Sin preparación: 6 %	• Muy preparado: 40 % • Algo preparado: 53 % • Sin preparación: 6 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Priorizar la ciberseguridad para el presente y para lo que se viene			
Las 3 principales soluciones de TI adoptadas para permitir el trabajo remoto	· Herramientas de colaboración: 81 % · Medidas de ciberseguridad: 65 % · Uso compartido de documentos en la nube: 64 %	· Herramientas de colaboración: 73 % · Medidas de ciberseguridad: 68 % · Uso compartido de documentos en la nube: 64 %	· Herramientas de colaboración: 73 % · Medidas de ciberseguridad: 68 % · Uso compartido de documentos en la nube: 63 %
Soluciones de TI adoptadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Medidas de ciberseguridad: 56 % · Herramientas de colaboración: 42 % · Protección de datos distribuidos: 29 %	· Medidas de ciberseguridad: 57 % · Herramientas de colaboración: 36 % · Protección de datos distribuidos: 23 %	· Medidas de ciberseguridad: 52 % · Herramientas de colaboración: 41 % · Servicios profesionales: 27 %
Los 3 principales cambios en las políticas de ciberseguridad para permitir el trabajo remoto	· Protección de terminales y mayor capacidad de VPN: 67 % · Mayores controles web y política de uso aceptable: 61 %	· Mayor capacidad de VPN: 64 % · Mayores controles web y política de uso aceptable: 57 % · Implementación de autenticación de varios factores: 51 %	· Mayor capacidad de VPN: 59 % · Mayores controles web y política de uso aceptable: 55 % · Implementación de autenticación de varios factores: 53 %
Proporción de cambios permanentes en las políticas de ciberseguridad	· 30 % o menos: 46 % · Más del 30 %: 51 %	· 30 % o menos: 44 % · Más del 30 %: 54 %	· 30 % o menos: 50 % · Más del 30 %: 45 %
Los 3 desafíos principales en la aplicación de los protocolos de ciberseguridad	· Falta de conocimiento o capacitación de los empleados: 63 % · Demasiadas herramientas o soluciones que utilizar y administrar: 50 % · Interfaces dispares: 34 %	· Falta de conocimiento o capacitación de los empleados: 58 % · Demasiadas herramientas o soluciones que utilizar y administrar: 49 % · Interfaces dispares: 33 %	· Falta de conocimiento o capacitación de los empleados: 59 % · Demasiadas herramientas o soluciones que utilizar y administrar: 50 % · Interfaces dispares: 35 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Inversiones en ciberseguridad en aumento			
Cambio en la inversión futura de la organización en ciberseguridad debido a la pandemia de COVID-19	· Aumento: 62 % · Disminución: 8 % · Sin cambios: 28 %	· Aumento: 68 % · Disminución: 7 % · Sin cambios: 23 %	· Aumento: 66 % · Disminución: 9 % · Sin cambios: 22 %
Proporción de aumento de la inversión futura en ciberseguridad	· 30 % o menos: 60 % · Más del 30 %: 36 %	· 30 % o menos: 56 % · Más del 30 %: 39 %	· 30 % o menos: 59 % · Más del 30 %: 36 %
Inversiones en ciberseguridad clasificadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Postura general de defensa en materia de ciberseguridad: 30 % · Seguridad en la nube: 28 % · Verificación de usuarios y dispositivos: 22 % · Acceso a la red: 20 %	· Postura general de defensa en materia de ciberseguridad: 31 % · Seguridad en la nube: 25 % · Acceso a la red Y verificación de usuarios y dispositivos: 22 %	· Postura general de defensa en materia de ciberseguridad: 34 % · Acceso a la red: 24 % · Seguridad en la nube: 22 % · Verificación de usuarios y dispositivos: 20 %

Estados Unidos

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
La importancia de la ciberseguridad en un futuro laboral híbrido			
Porcentaje de organizaciones con ***más de la mitad*** de la fuerza laboral trabajando en modalidad remota	· Antes de la COVID-19: 32 % · Durante la COVID-19: 71 % · Después de la COVID-19: 50 %	· Antes de la COVID-19: 24 % · Durante la COVID-19: 75 % · Después de la COVID-19: 46 %	· Antes de la COVID-19: 19 % · Durante la COVID-19: 62 % · Después de la COVID-19: 37 %
Importancia de la ciberseguridad para las organizaciones	· Sumamente importante: 43 % · Más importante que antes: 39 % · Algo importante: 17 %	· Sumamente importante: 50 % · Más importante que antes: 38 % · Algo importante: 11 %	· Sumamente importante: 44 % · Más importante que antes: 41 % · Algo importante: 15 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Un repunte resiliente: abordar las amenazas y los desafíos en materia de ciberseguridad			
Nivel de aumento de amenazas y alertas cibernéticas	• Aumento del 25 % o más: 54 % • No sabe: 10 %	• Aumento del 25 % o más: 64 % • No sabe: 5 %	• Aumento del 25 % o más: 61 % • No sabe: 8 %
Los 3 principales desafíos de ciberseguridad	• Acceso seguro: 59 % • Mantenimiento de políticas de control y aplicación: 48 % • Privacidad de los datos: 43 %	• Acceso seguro: 61 % • Privacidad de los datos: 56 % • Mantenimiento de políticas de control y aplicación: 53 %	• Acceso seguro: 62 % • Privacidad de los datos: 55 % • Mantenimiento de políticas de control y aplicación: 50 %
Aspecto difícil de proteger en un entorno remoto	• Computadoras portátiles o de escritorio de la oficina: 53 % • Dispositivos personales: 48 % • Aplicaciones en la nube: 39 % • Información de los clientes: 35 %	• Computadoras portátiles o de escritorio de la oficina: 59 % • Dispositivos personales: 52 % • Información de los clientes: 48 % • Aplicaciones en la nube: 46 %	• Computadoras portátiles o de escritorio de la oficina: 56 % • Dispositivos personales: 54 % • Información de los clientes Y aplicaciones en la nube: 46 %
Preparación para la transición a un entorno de trabajo remoto al comienzo de la pandemia de COVID-19	• Muy preparado: 46 % • Algo preparado: 48 % • Sin preparación: 6 %	• Muy preparado: 39 % • Algo preparado: 55 % • Sin preparación: 6 %	• Muy preparado: 40 % • Algo preparado: 53 % • Sin preparación: 6 %
Priorizar la ciberseguridad para el presente y para lo que se viene			
Las 3 principales soluciones de TI adoptadas para permitir el trabajo remoto	• Herramientas de colaboración y medidas de ciberseguridad: 64 % • Uso compartido de documentos en la nube: 49 %	• Herramientas de colaboración: 73 % • Medidas de ciberseguridad: 68 % • Uso compartido de documentos en la nube: 64 %	• Herramientas de colaboración: 73 % • Medidas de ciberseguridad: 68 % • Uso compartido de documentos en la nube: 63 %
Soluciones de TI adoptadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	• Medidas de ciberseguridad: 62 % • Herramientas de colaboración: 42 % • Servicios profesionales: 26 %	• Medidas de ciberseguridad: 57 % • Herramientas de colaboración: 36 % • Protección de datos distribuidos: 23 %	• Medidas de ciberseguridad: 52 % • Herramientas de colaboración: 41 % • Servicios profesionales: 27 %

Parámetros de investigación	Porcentaje del país	Promedio regional	Promedio global
Los 3 principales cambios en las políticas de ciberseguridad para permitir el trabajo remoto	· Mayor capacidad de VPN: 53 % · Implementación de autenticación de varios factores: 44 % · Mayores controles web y política de uso aceptable: 41 %	· Mayor capacidad de VPN: 64 % · Mayores controles web y política de uso aceptable: 57 % · Implementación de autenticación de varios factores: 51 %	· Mayor capacidad de VPN: 59 % · Mayores controles web y política de uso aceptable: 55 % · Implementación de autenticación de varios factores: 53 %
Proporción de cambios permanentes en las políticas de ciberseguridad	· 30 % o menos: 36 % · Más del 30 %: 59 %	· 30 % o menos: 44 % · Más del 30 %: 4 %	· 30 % o menos: 50 % · Más del 30 %: 45 %
Los 3 desafíos principales en la aplicación de los protocolos de ciberseguridad	· Falta de conocimiento o capacitación de los empleados: 56 % · Demasiadas herramientas o soluciones que utilizar y administrar: 35 % · Interfaces dispares: 32 %	· Falta de conocimiento o capacitación de los empleados: 58 % · Demasiadas herramientas o soluciones que utilizar y administrar: 49 % · Interfaces dispares: 33 %	· Falta de conocimiento o capacitación de los empleados: 59 % · Demasiadas herramientas o soluciones que utilizar y administrar: 50 % · Interfaces dispares: 35 %
Inversiones en ciberseguridad en aumento			
Cambio en la inversión futura de la organización en ciberseguridad debido a la pandemia de COVID-19	· Aumento: 57 % · Disminución: 8 % · Sin cambios: 31 %	· Aumento: 68 % · Disminución: 7 % · Sin cambios: 23 %	· Aumento: 66 % · Disminución: 9 % · Sin cambios: 22 %
Proporción de aumento de la inversión futura en ciberseguridad	· 30 % o menos: 49 % · Más del 30 %: 40 %	· 30 % o menos: 56 % · Más del 30 %: 39 %	· 30 % o menos: 59 % · Más del 30 %: 36 %
Inversiones en ciberseguridad clasificadas en orden de importancia (porcentaje de organizaciones que las clasificaron en primer lugar)	· Acceso a la red y postura general de defensa en materia de ciberseguridad: 30 % · Verificación de usuarios y dispositivos: 21 % · Seguridad en la nube: 19 %	· Postura general de defensa en materia de ciberseguridad: 31 % · Seguridad en la nube: 25 % · Acceso a la red Y verificación de usuarios y dispositivos: 22 %	· Postura general de defensa en materia de ciberseguridad: 34 % · Acceso a la red: 24 % · Seguridad en la nube: 22 % · Verificación de usuarios y dispositivos: 20 %

INFORME ACERCA DEL FUTURO DEL TRABAJO REMOTO SEGURO

En febrero y marzo de 2020, las organizaciones buscaron proteger su fuerza laboral exigiendo y permitiendo que los empleados trabajen desde su casa. Si bien era necesaria para proteger a las personas y las comunidades, esta experiencia separó físicamente a los profesionales de seguridad de sus propios equipos, de los empleados que dependían de ellos y de los sistemas críticos de los que eran responsables. El acuerdo de trabajo remoto también ejerció mayor presión sobre las políticas digitales existentes y la planificación de la continuidad del negocio durante un momento ya de por sí estresante.

Esto no quiere decir que no hayamos podido encontrar maneras de adaptarnos a esta nueva forma de trabajar. En el contexto de esta realidad, se encuestó a más de 3000 responsables de la toma de decisiones de TI de organizaciones pequeñas a grandes entre el 16 de junio y el 4 de septiembre de 2020, dentro de un espectro de 30 sectores —entre ellos, los servicios financieros, los servicios de salud, la arquitectura, el transporte, etc.— para comprender cómo se vieron afectados por la crisis de COVID-19 desde el punto de vista de la seguridad cibernética.

3196 encuestados en **21** mercados

América:
- Brasil
- Canadá
- México
- Estados Unidos

Europa:
- Francia
- Alemania
- Italia
- Reino Unido

APJC:
- Australia
- China
- Hong Kong
- India
- Indonesia
- Japón
- Corea
- Malasia
- Filipinas
- Singapur
- Taiwán
- Tailandia
- Vietnam

Sectores:
- Contabilidad
- Arquitectura
- Asesoramiento comercial
- Fabricación o ingeniería química
- Construcción
- Educación
- Servicios financieros
- Gobierno
- Atención médica
- Fabricación:
- no relacionada con la informática
- Comercio minorista
- Desarrollo de software
- Telecomunicaciones
- Transporte
- Comercio mayorista y distribución
- De beneficencia/sin fines de lucro

Público:
Profesionales responsables del área de TI de su empresa

Estas organizaciones incluyen:
- pequeñas (entre 1 y 249 empleados),
- medianas (entre 250 y 999 empleados), y
- grandes empresas (1000 empleados o más).

Objetivos:

- Explorar los **desafíos** que implica trasladar parte o la totalidad de la fuerza laboral de una organización a un **entorno remoto** de la noche a la mañana y la **preparación** de las organizaciones de todo el mundo para proteger sus negocios en un acuerdo de trabajo remoto

- Comprender cómo se adaptaron las empresas a esta transición repentina, incluidos los cambios en sus prioridades, políticas e inversiones en ciberseguridad

- Permitir que las empresas comprendan y se preparen para un entorno de trabajo híbrido mediante una adaptación segura a fin de protegerse en el presente y en el futuro

Parámetros de investigación

N.º 1 El aumento de trabajadores remotos durante la pandemia de COVID-19 y la importancia de la ciberseguridad para respaldarlos

1) Cantidad de trabajadores remotos antes, durante y después de la pandemia de COVID-19
2) Importancia de la ciberseguridad en el panorama actual del trabajo remoto durante la pandemia de COVID-19

N.º 2 Abordar la preparación, las amenazas y los desafíos de ciberseguridad

1) Cuál es el nivel de las organizaciones, con sus funciones y soluciones de ciberseguridad, para hacer la transición —repentina— al trabajo remoto
2) Tipos de desafíos de ciberseguridad encontrados durante el trabajo remoto masivo y su gravedad en orden de importancia
3) Lo más difícil de proteger durante el trabajo remoto

N.º 3 Prioridades y adopción de tecnología para respaldar el trabajo remoto

1) Tipo de tecnologías adoptadas
2) Clasificación y orden de importancia de las tecnologías adoptadas

N.º 4 Movimientos en las políticas de ciberseguridad y los protocolos de aplicación para respaldar a los trabajadores remotos

1) Tipo de cambios realizados
2) Proporción de cambios en las políticas de ciberseguridad
3) Desafíos en la aplicación de los protocolos de ciberseguridad

N.º 5 Inversiones en ciberseguridad, hoy y en adelante

1) Si la pandemia de COVID-19 cambiará la inversión futura en ciberseguridad de la organización
2) Porcentaje de aumento, disminución o ausencia de cambios en la inversión
3) Clasificación de la inversión futura en ciberseguridad en orden de importancia

El futuro del trabajo remoto seguro

cisco SECURE