ivanti

Informe De Ciberseguridad Del Teletrabajo

2020

Visión General

Las soluciones de acceso seguro mantienen a las empresas en funcionamiento al permitir la informática a distancia segura y conectar a las personas y los dispositivos con el centro de datos y las aplicaciones en la nube, incluso durante las circunstancias más impredecibles.

A medida que el impacto del Coronavirus (COVID-19) se intensificó y se convertía en una pandemia, la Organización Mundial de la Salud sugirió que los ciudadanos trabajaran desde sus casas y evitaran utilizar el transporte público y los entornos de oficina como medida de precaución para así, mitigar la propagación y el riesgo de infección.

A principios de 2020, funcionarios gubernamentales y locales de todo el mundo empezaron a aconsejar y a exigir a los ciudadanos que se confinaran en sus hogares y dejaran de trabajar en sus locales, excepto en los negocios esenciales. Las empresas iniciaron acciones inmediatas para ampliar y facilitar el teletrabajo.

Además de afectar potencialmente a la productividad de los usuarios, este cambio de emergencia en el lugar de trabajo y la rápida necesidad de capacidad de trabajo a distancia amenazaron la infraestructura de TI, la continuidad del negocio y la seguridad de la información.

Este informe sobre el teletrabajo en 2020, patrocinado por Pulse Secure y llevado a cabo por Cybersecurity Insiders, ofrece una perspectiva en profundidad sobre cómo las empresas realizaron la transición de los trabajadores y los recursos, y revela los desafíos, las preocupaciones, las estrategias y los resultados previstos en materia de ciberseguridad del trabajo a distancia. La encuesta, realizada en mayo de 2020, encuestó a más de 400 responsables de la toma de decisiones en materia de seguridad informática, profesionales y empresas de distintos tamaños de múltiples sectores. La encuesta reveló que el 84 % de las empresas prevén un trabajo remoto más amplio y permanente y casi un tercio planea aumentar su presupuesto para el acceso seguro a corto plazo.

Las principales conclusiones son:

La capacidad de los usuarios que teletrabajan ha aumentado más de 3 veces, con más del 75 % de las organizaciones ofreciendo una cobertura de casi el 100 %

El 33 % de las empresas no estaban suficientemente preparadas para el acceso a distancia de forma segura e imprevista

El 54 % acelerará más flujos de trabajo y aplicaciones a la nube

El 38 % de las organizaciones experimentó un aumento de la productividad y otros beneficios

El 84 % anticipa programas de teletrabajo más amplios y permanentes

Más de la mitad prevé aumentar un presupuesto de acceso seguro en los próximos doce meses (a partir de abril de 2020)

El 66 % espera que aumenten las amenazas a la seguridad del teletrabajo y el 63 % prevé que el teletrabajo podría exponer riesgos de cumplimiento.

El malware, la suplantación de identidad, el acceso no autorizado de usuarios y dispositivos, y los sistemas sin parches fueron percibidos como los vectores de ataque más importantes del trabajo a distancia.

El antivirus/malware, el cortafuegos, la VPN SSL, la autenticación multifactor y las copias de seguridad fueron las principales soluciones empleadas para garantizar la seguridad/resiliencia de la empresa.

Muchas gracias a Pulse Secure por apoyar este importante proyecto de investigación.

Esperamos que este informe le resulte informativo y útil en sus esfuerzos por proteger sus inversiones en TI, garantizar la continuidad del negocio y proteger a sus empleados.

Gracias,

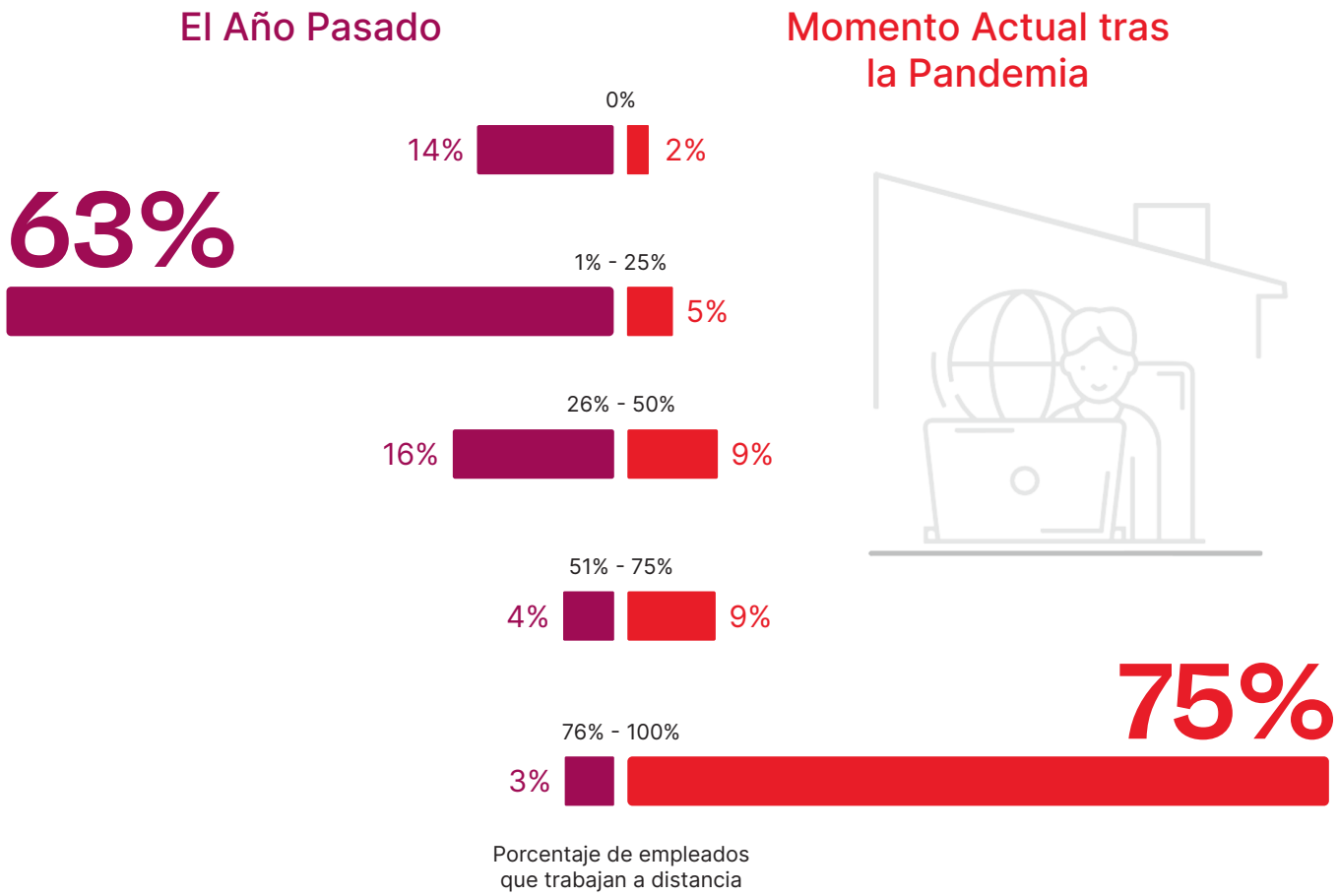
Holger Schulze

CEO y fundador de
Cybersecurity Insiders

El Insólito Aumento Del Teletrabajo

La encuesta revela un cambio masivo hacia entornos de trabajo a distancia y en casa debido a la pandemia del COVID-19. Mientras que una mayoría del 63 % de las empresas tenía hasta una cuarta parte de los empleados trabajando en entornos remotos/ en casa antes de la crisis, tres cuartas partes de las mismas organizaciones informan de que más del 75 % de su plantilla trabaja ahora desde

¿Qué porcentaje de su plantilla ha trabajado a distancia o en casa EL AÑO PASADO en comparación con EL MOMENTO ACTUAL durante la crisis de COVID?

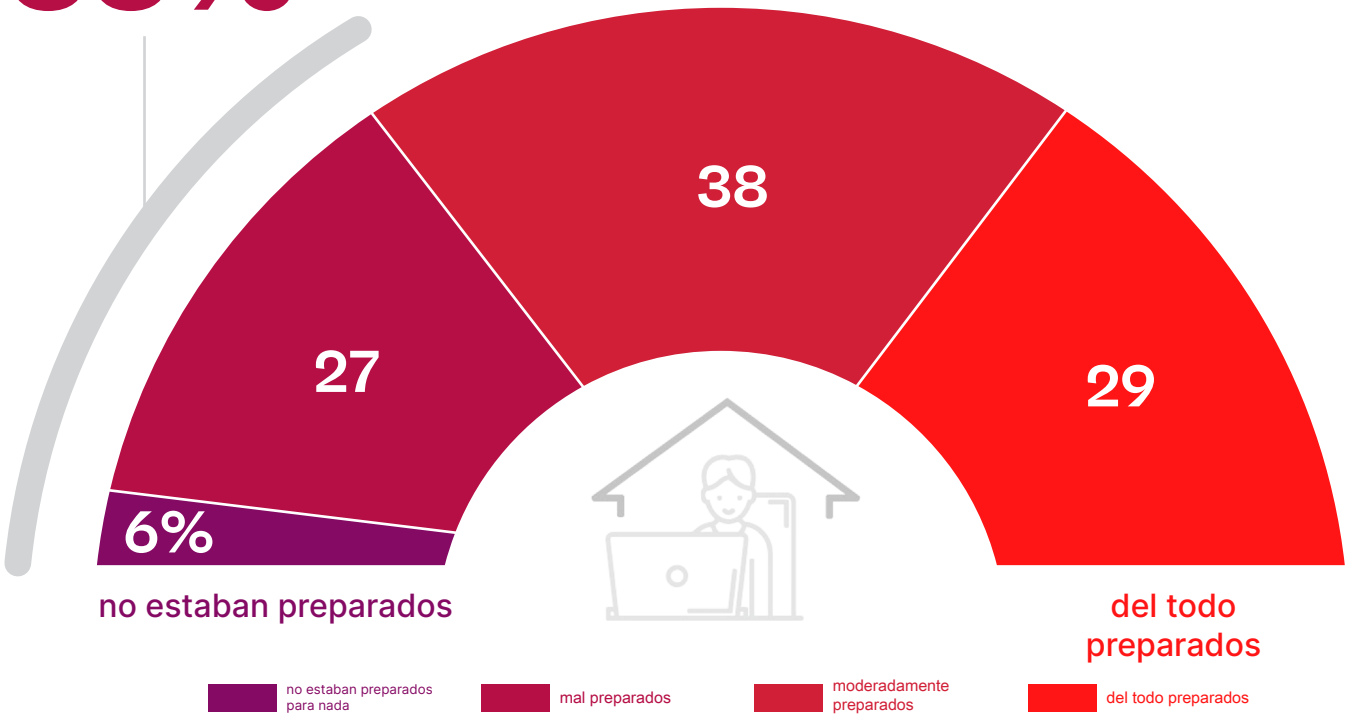


La Capacidad De Implantar El Teletrabajo

Un tercio de las compañías revelan que no estaban suficientemente preparadas para el cambio inminente de las instalaciones a los escenarios del trabajo a distancia.

Antes de la pandemia de COVID-19, ¿hasta qué punto estaba preparada su organización con un plan de continuidad de la actividad/recuperación de desastres que incluyera un cambio inminente de la mano de obra local a la remota?

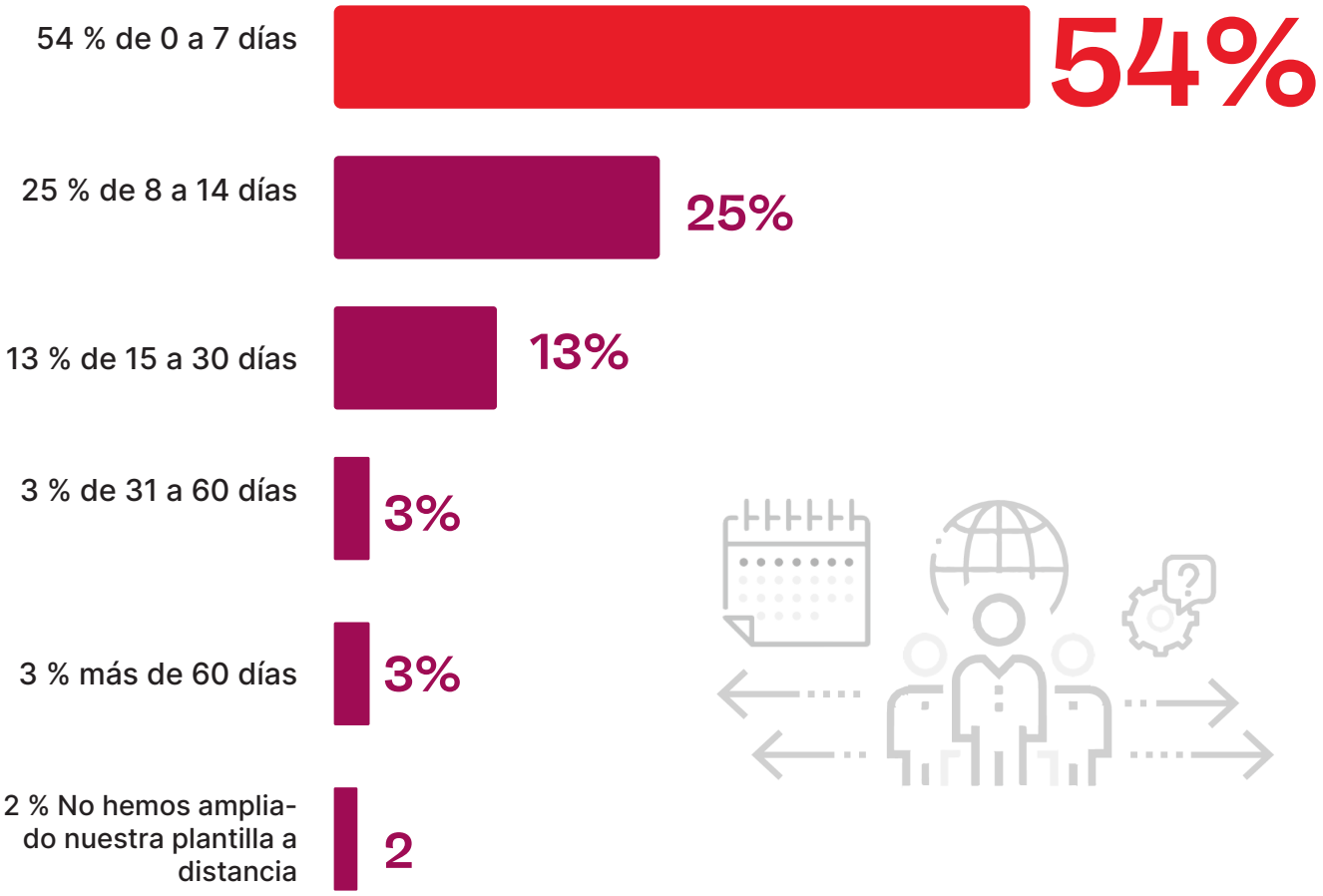
33% De las organizaciones informan que no estaban suficientemente preparadas.



Días Para Ampliar La Capacidad Del Teletrabajo

Una mayoría de empresas (54%) afirma haber ampliado con éxito la capacidad de teletrabajar en siete días o menos.

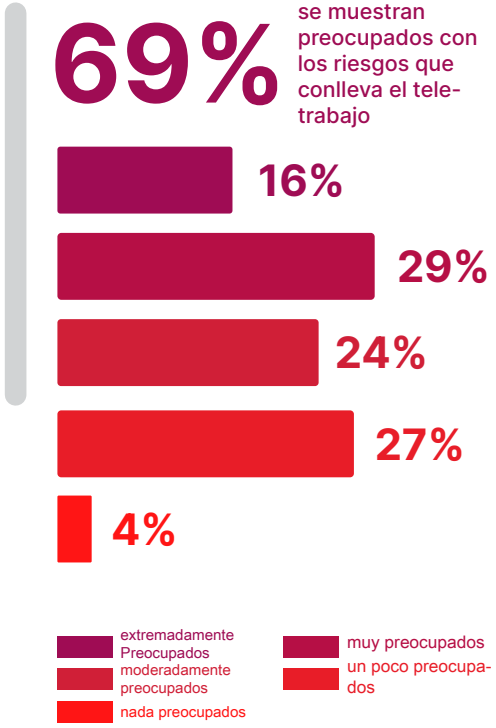
¿Cuántos días tardó su organización en ampliar su capacidad para dar pleno apoyo al personal remoto recientemente ampliado?



Percepciones De Seguridad En El Teletrabajo

Mientras que el 79 % de las organizaciones creen que tienen una preparación adecuada en materia de seguridad en trabajo remoto, dos tercios de las organizaciones de esta encuesta (69 %) están preocupadas por los riesgos de seguridad de los usuarios que trabajan desde casa.

¿Hasta qué punto le preocupan los riesgos de seguridad introducidos por los usuarios que trabajan desde casa y hasta qué punto estaba preparada su organización para el cambio al trabajo a distancia desde el punto de vista de la seguridad?



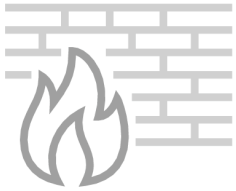
Controles De Seguridad Establecidos

Los principales controles de seguridad para proteger el trabajo a distancia/desde casa son las soluciones antivirus y antimalware (77 %), firewall (77 %), las redes privadas virtuales (66 %) y la autenticación multifactor (66 %).

¿Qué controles de seguridad aplica actualmente para asegurar los escenarios de trabajo remoto en casa?

77%

antivirus / antimalware



77%

Firewall

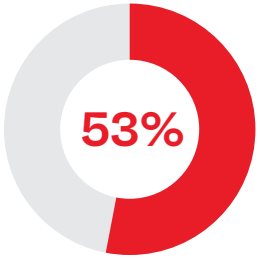
66%

red virtual privada
(VPN/SSL-VPN)

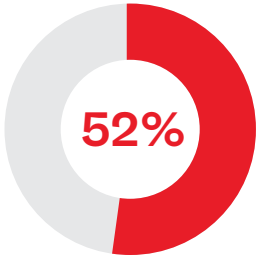
66%

autenticación multifactor
(MFA)

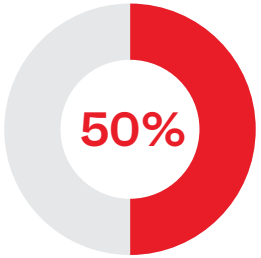
Antiphishing 47 % | Inicio de sesión único 45 % | Cumplimiento de puntos finales 34 % | Gestión de dispositivos móviles (MDM) 34 % | Firewall de aplicaciones web 29 % | Infraestructura de escritorio virtual (VDI) 26 % | Equilibrio de carga/Controlador de entrega de aplicaciones (ADC) 24 % | Proxy web/filtrado web 23 % | Cloud DLP 18 % | Cloud Access Security Brokers (CASB) 16 % | Supervisión del comportamiento de usuarios y entidades (UEBA) 11% | Perímetro definido por software (SDP) 10 % | Acceso a la red de confianza cero (ZTNA) 8 % | Otros 3 %. Perímetro Definido por Software (SDP) 10 % | Acceso a la Red de Confianza Cero (ZTNA) 8 % | Otros 3 %



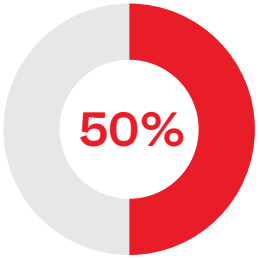
copia de seguridad y recuperación



gestión de contraseña



codificación de archivos



seguridad de puntos finales
(EDR)

Principales Retos De Seguridad

La concientización de los usuarios ocupa el primer lugar (59 %) en la lista de los principales retos de seguridad a los que se enfrentan las organizaciones que están aumentando sus plantillas remotas. Le siguen el acceso a través de redes domésticas o públicas no seguras (56 %) y el uso de dispositivos personales (43 %).

¿Cuál considera que es el mayor reto de seguridad de su organización en relación con el aumento de la mano de obra a distancia? 59 % Sensibilización de los usuarios y formación

59%

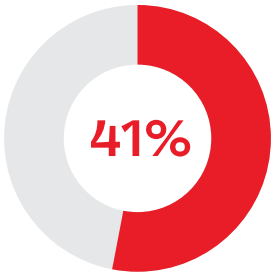
Sensibilización de los usuarios

56%

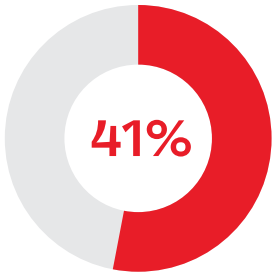
Seguridad de la red wifi pública o del hogar

43%

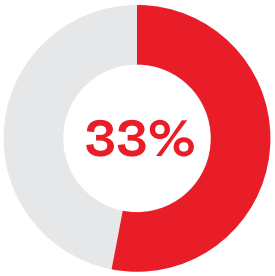
Uso de dispositivos personales/BYOD



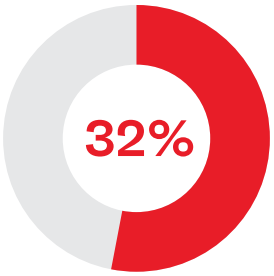
Datos sensibles fuera del perímetro



Aumento de riesgos de seguridad



La falta de visibilidad



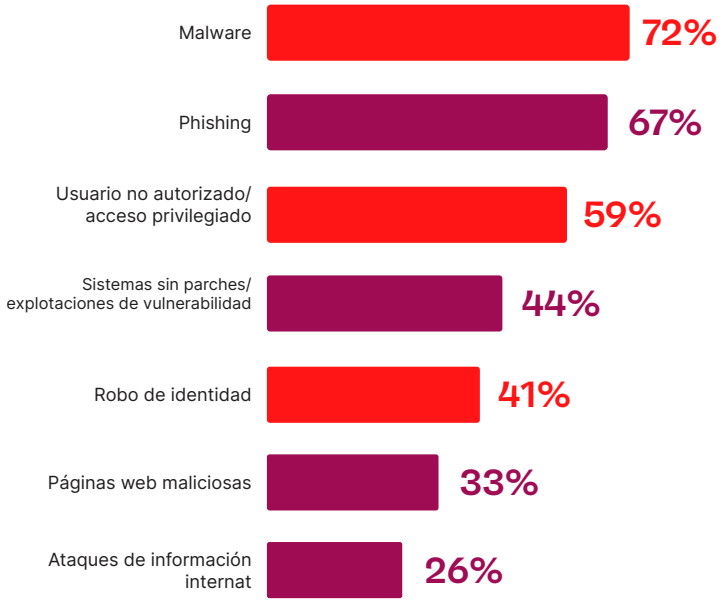
Coste adicional de soluciones de seguridad

Disponibilidad/experiencia del usuario 30 % | Añadir capacidad 24 % | Uso no autorizado de aplicaciones en la nube 21 % | Lagunas de responsabilidad/auditoría

Vectores De Ataque Ampliados

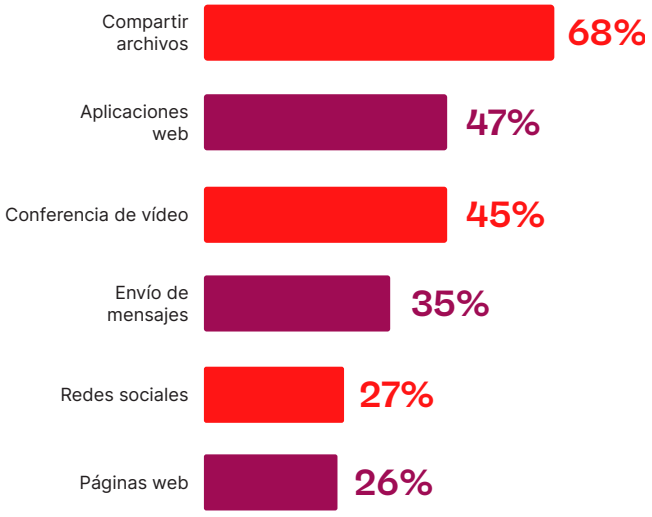
El malware, el phishing, el acceso no autorizado de usuarios/dispositivos y los sistemas sin parches fueron identificados como los principales vectores de ataque debido a que los empleados trabajan desde casa. Entre las aplicaciones que contribuyen a la productividad y la colaboración, las organizaciones son las que más preocupan por la seguridad a la hora de compartir archivos (68 %), las aplicaciones web (47 %), las videoconferencias

¿Qué vectores de amenaza específicos le preocupan más con los empleados que trabajan desde casa?



Incerto 5%

¿Qué aplicaciones de trabajo utilizadas por los trabajadores remotos le preocupan más desde el punto de vista de la seguridad?



Altro 2%

Nivel De Seguridad Del Teletrabajo

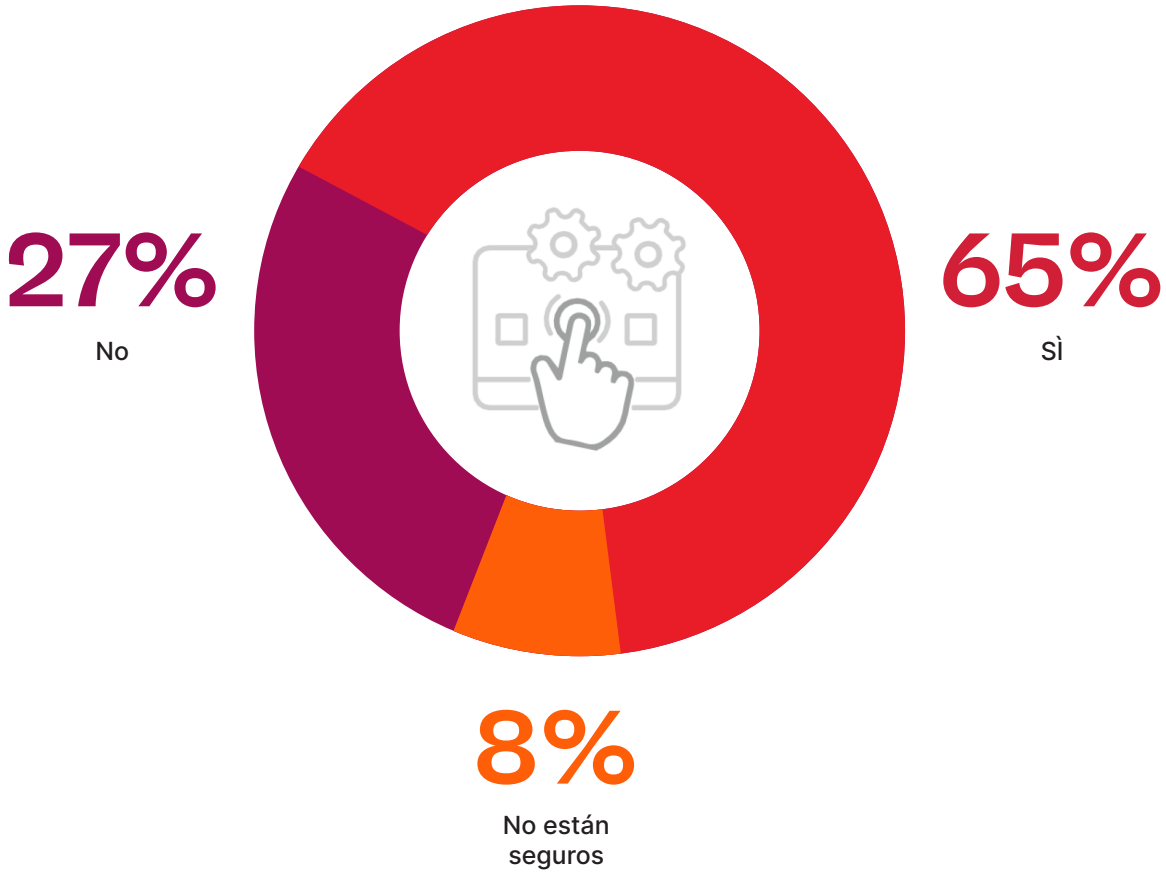
Una mayoría del 78 % confirma que aplica el mismo nivel de controles de seguridad para todas las funciones a las que se accede de forma remota.

¿Impone el mismo nivel de controles de seguridad y gestión de datos para todos los roles de la empresa que acceden de forma remota?

Acceso Desde Dispositivos Personales

Casi tres cuartas partes de las organizaciones permiten el acceso desde dispositivos personales no gestionados para apoyar el trabajo desde casa, mientras que al menos el 27 % ve este escenario como un riesgo de seguridad importante.

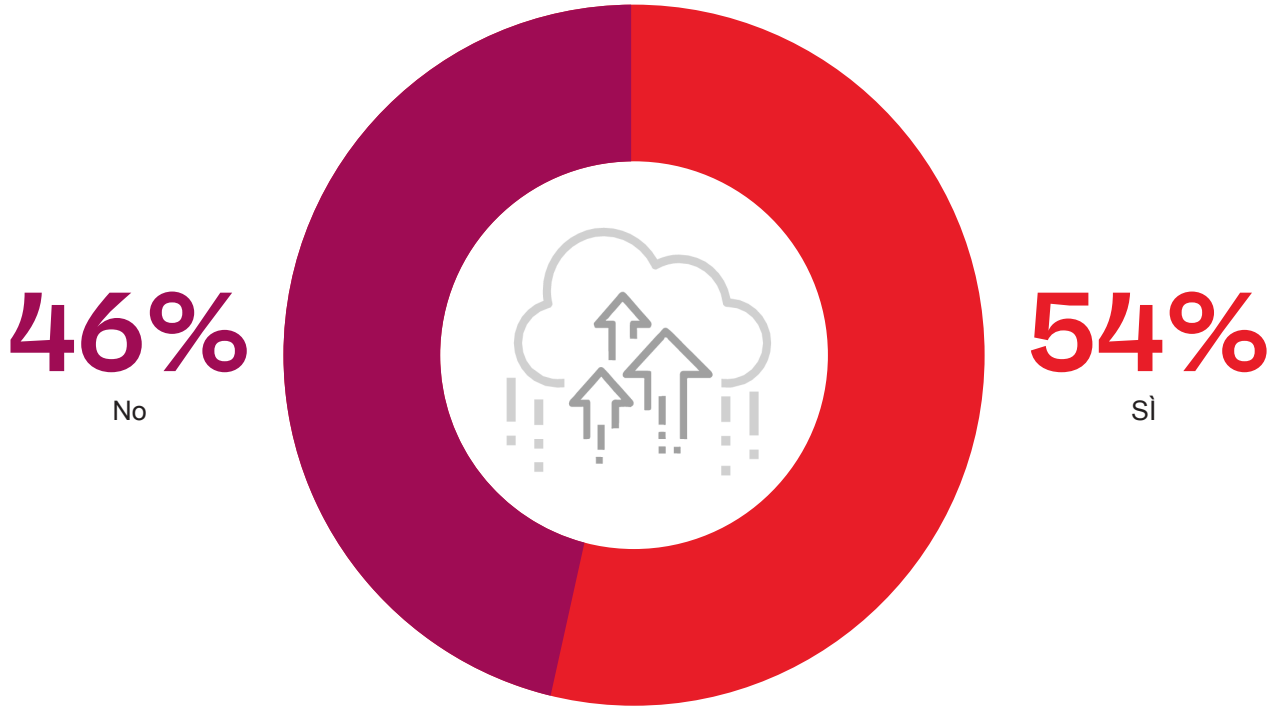
¿Pueden los empleados acceder a las aplicaciones gestionadas desde dispositivos personales no gestionados?



Migración A La Nube

Una mayoría del 54 % confirma que la pandemia de COVID aceleró la migración de los flujos de trabajo a las aplicaciones basadas en la nube.

¿Ha acelerado COVID la migración de flujos de trabajo o aplicaciones de usuarios adicionales a aplicaciones basadas en la nube?



Riesgo De Seguridad A Distancia

Las organizaciones están más preocupadas por la protección de los datos sensibles, especialmente cuando se accede a ellos a través de puntos finales no gestionados (46%), seguido de la mayor exposición al malware (34%).

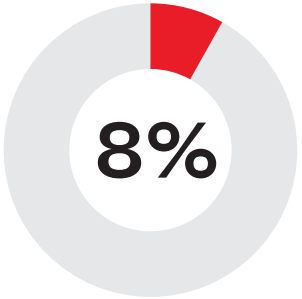
¿Cuál es el principal riesgo que le preocupa cuando sus usuarios se conectan a distancia?

46%

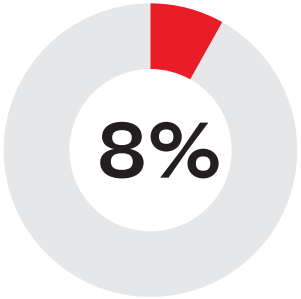
La protección de mis datos, especialmente cuando se accede a ellos mediante puntos finales no gestionados

34%

Exposición a malware, phishing u otros exploits



Garantizar el cumplimiento de mis usuarios regulados



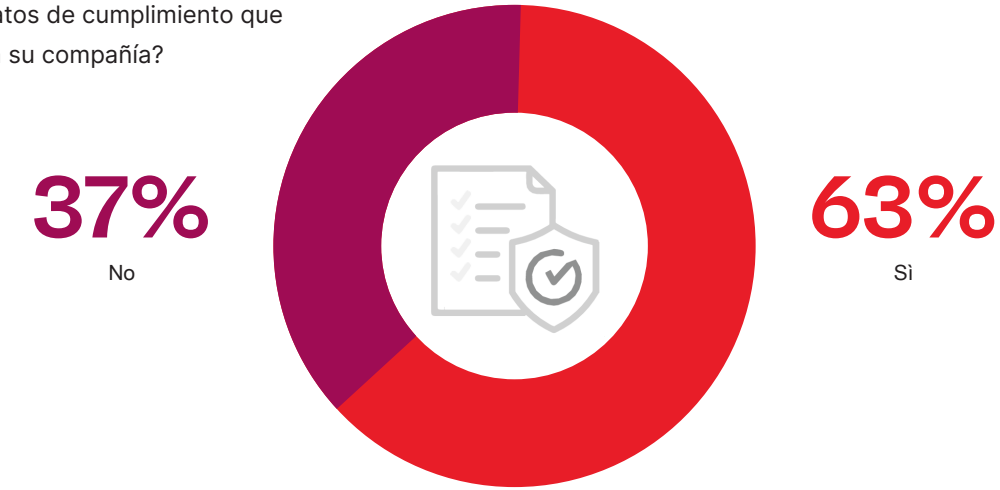
Auditoría y supervisión de empleados que realizan trabajos desde recursos no gestionados

Otros 4%

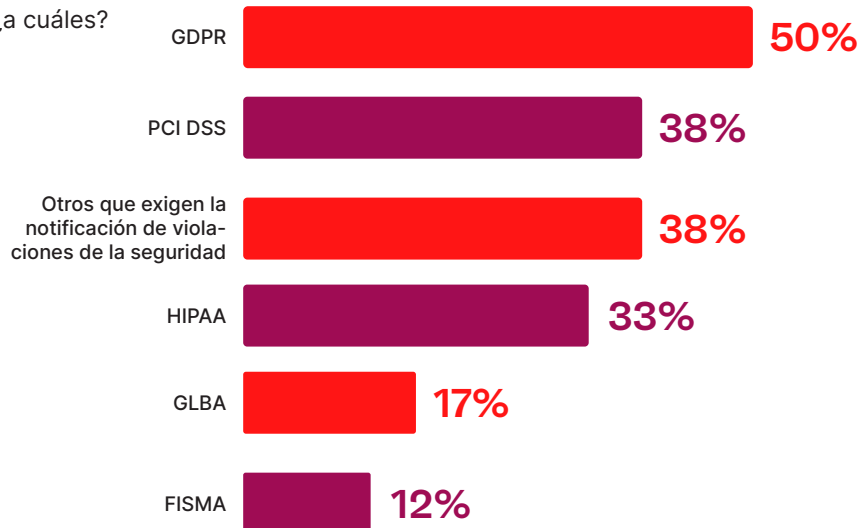
Impacto De Cumplimiento

Dos tercios de las organizaciones consideran que los entornos de trabajo remotos tienen un impacto en su postura de cumplimiento.

¿Podría el trabajo a distancia afectar a los mandatos de cumplimiento que se aplican a su compañía?



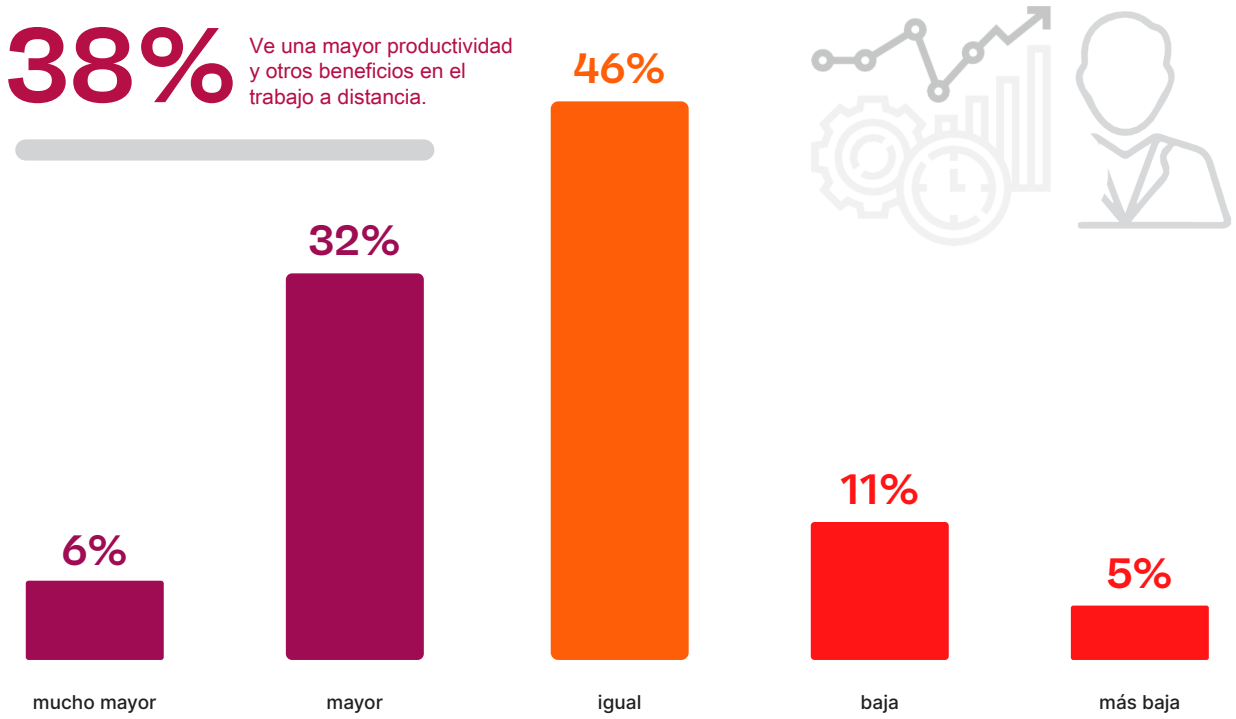
En caso afirmativo, ¿a cuáles?



Efectos De La Productividad

El 38 % de las organizaciones manifestaron que ven una mayor productividad y otros beneficios en el trabajo a distancia. Solo el 16 % ve una menor productividad.

¿Su organización está viendo una mayor productividad y otros beneficios en el trabajo a distancia?

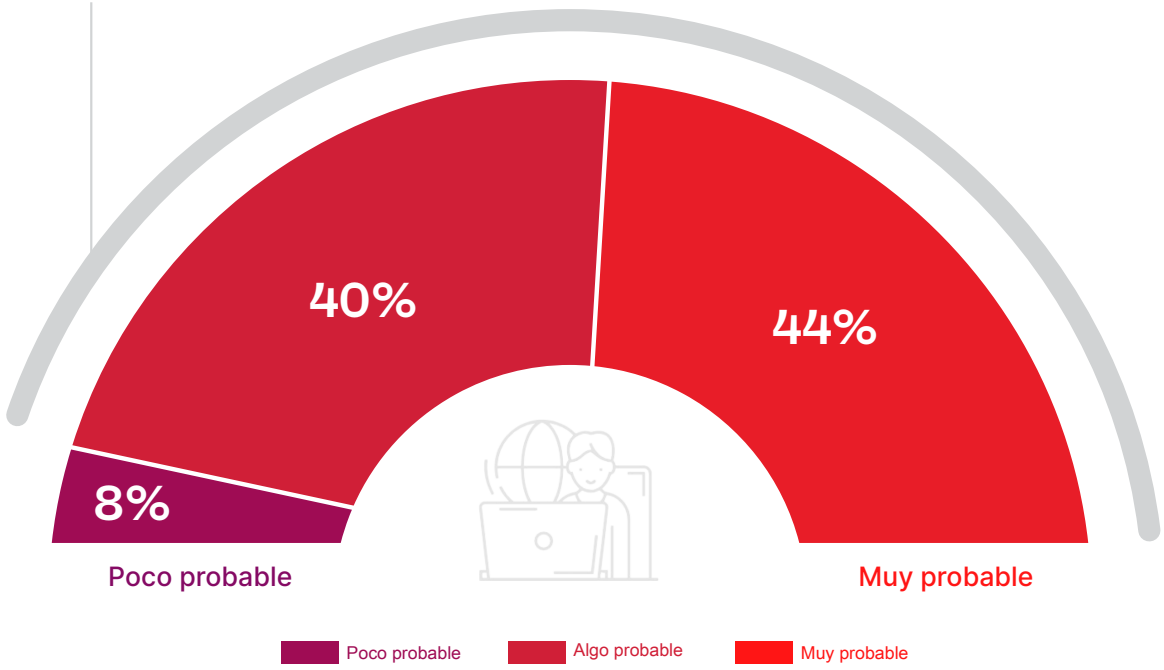


Futuro Teletrabajo

Una mayoría del 84 % de las organizaciones considera probable (el 44 % muy probable) que sigan aumentando las capacidades de trabajo desde casa en el futuro, aprovechando el aumento de la productividad y otras ventajas empresariales.

¿Espera seguir apoyando el aumento de las capacidades de trabajo desde casa en el futuro (debido al aumento de la productividad y otros beneficios empresariales)?

84% De las organizaciones consideran probable que sigan aumentando las capacidades de trabajo desde casa en el futuro.

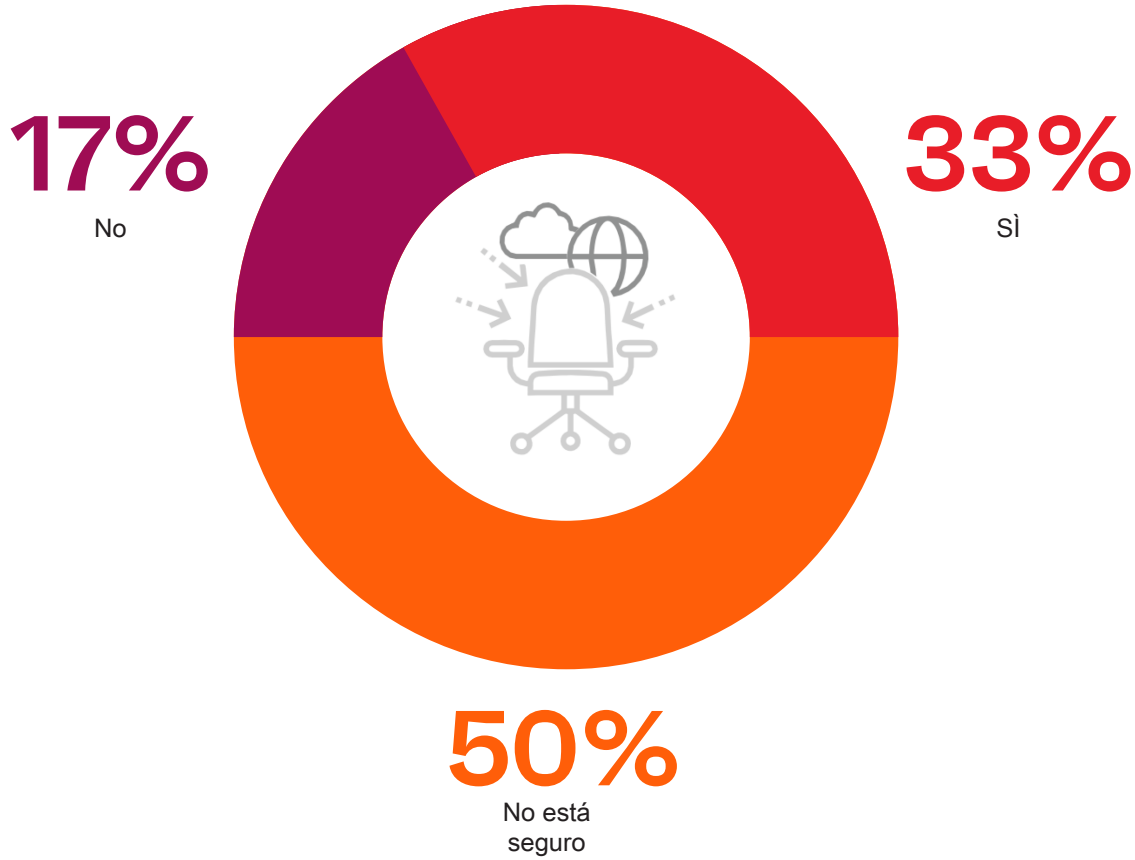


8 % No está seguro

El Teletrabajo Como Algo Permanente

Un tercio de las organizaciones está estudiando la posibilidad de hacer que algunos puestos sean permanentemente remotos cuando termine la crisis del COVID.

¿Su organización está considerando la posibilidad de hacer que algunos puestos sean permanentemente remotos (que solían ser presenciales) cuando termine la pandemia?

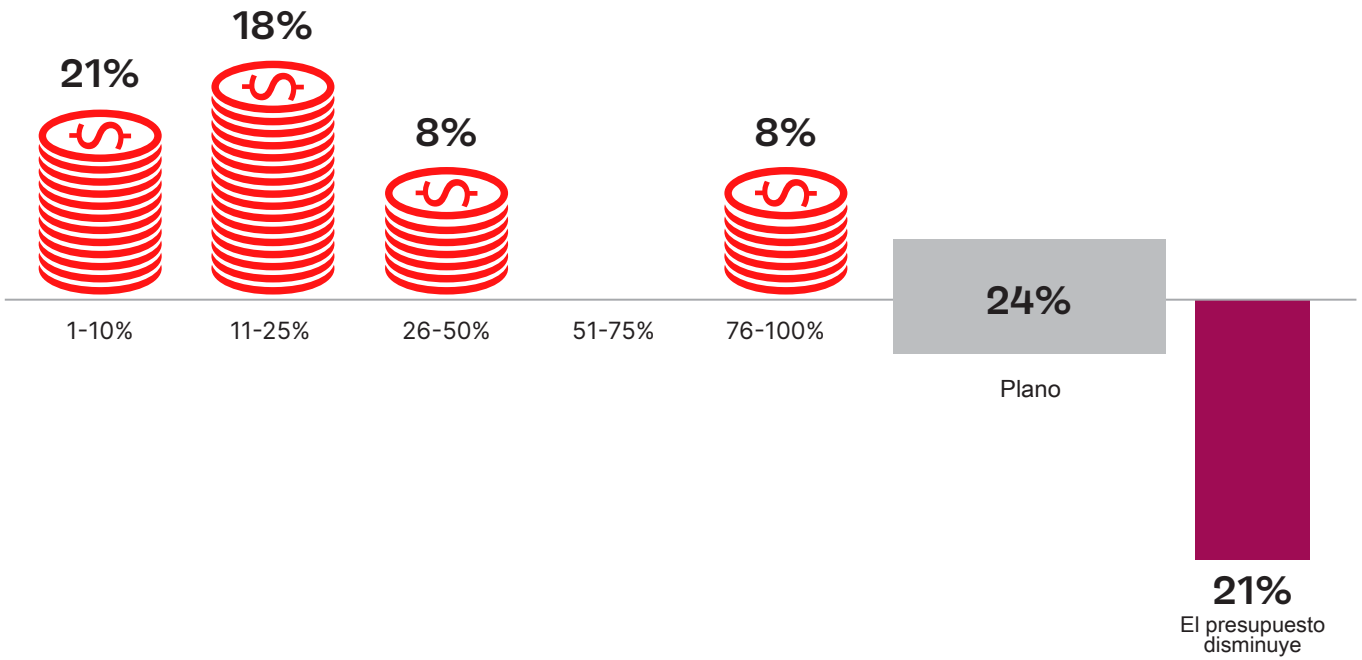


Tendencias Presupuestarias

La mayoría (55 %) de las organizaciones espera que los presupuestos para la seguridad del personal remoto aumenten en los próximos 12 meses (a partir de abril de 2020). Para una cuarta parte de los encuestados, estos presupuestos de seguridad se mantendrán sin cambios y solo el 21 % ve que los presupuestos se reducirán.

¿Cómo va a aumentar su presupuesto para los controles de seguridad del trabajo a distancia en los próximos 12 meses?

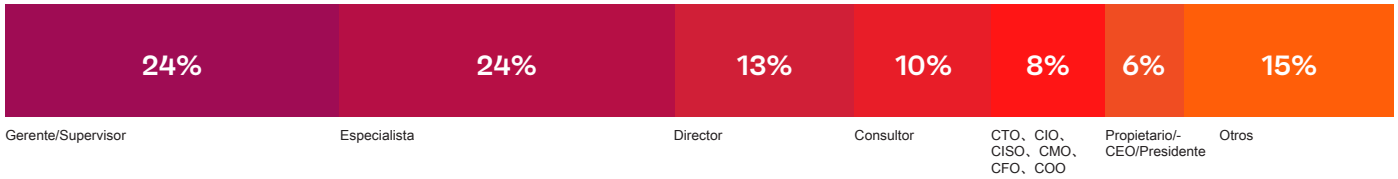
55% Se espera que los presupuestos para la seguridad de los trabajadores a distancia aumenten un 55% en los próximos 12 meses.



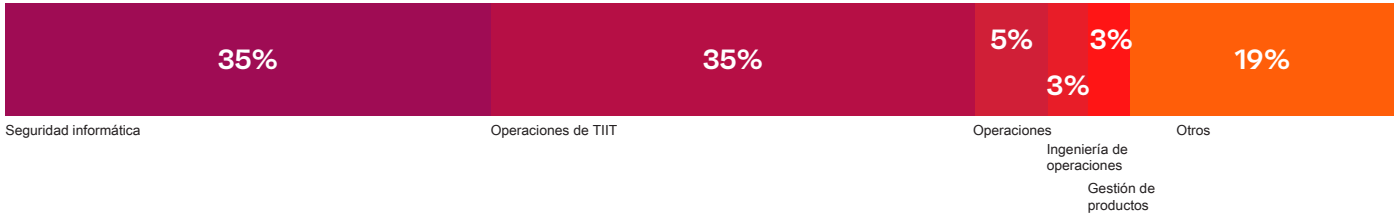
Metodología Y Datos Demográficos

Este informe se basa en los resultados de una exhaustiva encuesta en línea de 413 profesionales de TI y ciberseguridad en los EE.UU., realizada en mayo de 2020 para identificar las últimas tendencias de adopción de las empresas, los desafíos, las brechas y las preferencias de soluciones para las fuerzas de trabajo remotas a raíz de la pandemia de COVID-19 de 2020. Los encuestados van desde ejecutivos técnicos hasta profesionales de la seguridad de TI, representando una sección transversal equilibrada de organizaciones de diversos tamaños a través de múltiples industrias.

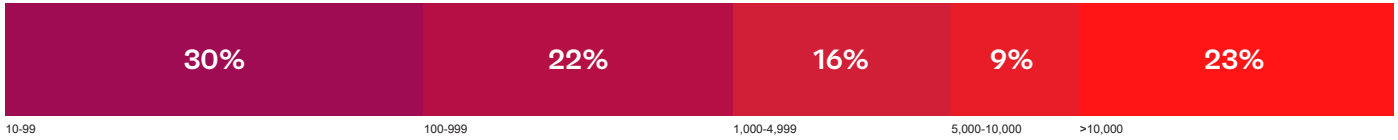
Nivel profesional



Sector



Tamaño de la empresa



Industria

Pulse Secure
Acquired by Ivanti

Pulse Secure ofrece soluciones de acceso seguro fáciles y completas basadas en software para personas, dispositivos, cosas y servicios que mejoran la visibilidad, la protección y la productividad de nuestros clientes. Nuestras suites integran de forma única el acceso a la nube, a los dispositivos móviles, a las aplicaciones y a la red para permitir la TI híbrida en un mundo de confianza cero. Más de 23.000 empresas y proveedores de servicios de todos los sectores verticales confían en Pulse Secure para que su personal móvil pueda acceder de forma segura a las aplicaciones y a la información en el centro de datos y en la nube, garantizando al mismo tiempo el cumplimiento de la normativa empresarial. Más información en www.pulsesecure.net

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com