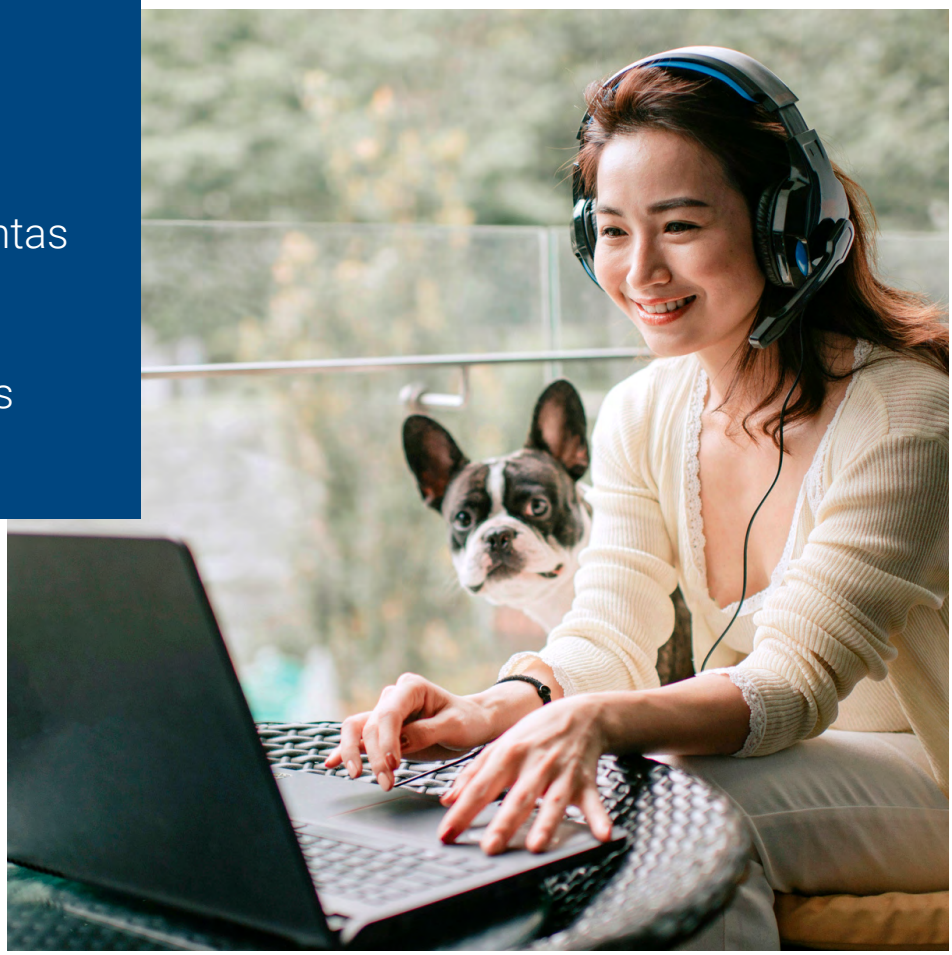
El nuevo mundo del teletrabajo: Las nuevas herramientas para asistir a los empleados de forma segura son esenciales



El teletrabajo es la nueva normalidad y está aquí para quedarse.

Según una encuesta de Gallup, alrededor del 24 % de los empleados dicen que esperan trabajar exclusivamente de forma remota a partir del 2022, mientras que el 53 % anticipa que trabajará de forma híbrida (tanto en la oficina como de forma remota). Para las empresas, este tipo de flexibilidad laboral es clave. De hecho, los empleados la demandan.

En medio de la Gran Renuncia, todos los profesionales tienen más opciones y están buscando oportunidades que les ofrezcan un mejor equilibrio entre el trabajo y el ocio. Las empresas que quieren tener éxito deben ofrecer y aceptar esta nueva realidad; les deben proporcionar a los empleados (incluidos los equipos de TI) las herramientas necesarias para cumplir sus responsabilidades sin importar dónde o cuándo estén trabajando. Al mismo tiempo, deben darle prioridad a la seguridad, ya que el volumen de violaciones de la ciberseguridad y el nivel de sofisticación no hacen más que crecer.

Por necesidad, durante la pandemia, muchas empresas tuvieron que improvisar soluciones precarias para gestionar el teletrabajo. Pero el número de aplicaciones implementadas como soluciones rápidas solo sirvieron para aumentar la carga de trabajo de los departamentos de TI, poniendo a prueba a los equipos que ya están bajo presión por la creciente complejidad de su trabajo y la escasez crónica de personal.

Las empresas de hoy en día necesitan un sistema eficiente y confiable que garantice la seguridad y la funcionalidad del teletrabajo, pero que también les ofrezca a los equipos de TI una forma más sofisticada de asistencia remota para gestionar la nueva fuerza laboral dispersa.

"La seguridad siempre fue un desafío subyacente", dice Michael Polaczy, director de marketing de productos en TeamViewer, "pero últimamente los obstáculos que hay que superar son más elevados. Con la fuerza de trabajo híbrida se viene todo un nuevo grupo de desafíos de seguridad".

Muchos empleados cambiaron cuándo y cómo hacen su trabajo, exigiendo una asistencia informática más frecuente y flexible.

Una multitud de nuevos desafíos

En el pasado, cuando muchas empresas trabajaban únicamente de forma presencial, los gerentes de TI solo tenían que enfocarse en asegurar su entorno local para proteger sus datos y su privacidad. Además, las configuraciones de TI en su mayoría estaban estandarizadas y el personal de TI podía acceder fácilmente a ellas para gestionarlas, darles mantenimiento y ofrecer asistencia. Ahora, el trabajo remoto e híbrido amplió enormemente el número y los tipos de ubicaciones que las empresas necesitan gestionar y proteger. Los empleados pueden trabajar desde la oficina corporativa, su casa, una habitación de hotel, un espacio de coworking o una cafetería, todos fuera de las instalaciones conocidas y seguras de la red de la empresa. Cada ubicación adicional se suma a la complejidad de un entorno de trabajo descentralizado y puede generar una pérdida de visibilidad crítica. Esta nueva realidad requiere un enfoque diferente de la gestión de activos y la protección de puntos finales.

Incluso, esos puntos finales abarcan toda esa diversidad: plataformas de escritorio y móviles, con las computadoras remotas, los smartphones, los servidores, las terminales de pago y los dispositivos del IoT, en cualquier momento y lugar. Esto se complica aún más: las políticas de "trae tu propio dispositivo" (BYOD, por sus siglas en inglés) amplían enormemente el número y el tipo de equipos diferentes que el departamento de TI debe asistir y proteger.

Las empresas pueden quedar vulnerables, sin saber qué programas utilizan los empleados en sus dispositivos personales y si esos programas cumplen o no las políticas internas de TI. Los equipos de TI necesitan capacidades de monitoreo remotas y seguras para saber qué empleados están utilizando aplicaciones y sistemas determinados, para tomar el control de su entorno de TI si es necesario y para detectar proactivamente los pequeños inconvenientes antes de que se conviertan en problemas graves.

"Cada aplicación adicional supone un nuevo riesgo de seguridad y eso aumenta las posibilidades de que se produzcan ciberataques y delitos por adversarios cibernéticos", dice Polaczy.

Las llamadas de servicio en el lugar solían ser la norma. Pero el entorno de trabajo híbrido actual depende de la capacidad del departamento de TI para brindar fácilmente un servicio de asistencia remota y segura para los dispositivos.

Muchos empleados cambiaron cuándo y cómo hacen su trabajo, exigiendo una asistencia informática más frecuente y flexible. Un empleado que trabaja de noche o durante un fin de semana puede necesitar que el departamento de TI solucione un problema al instante, lo que significa que el personal de TI debe estar más "de guardia" que nunca. En pocas palabras, lo que necesitan los equipos de TI es una forma rápida y sencilla de evaluar y solucionar los problemas para garantizar la continuidad del negocio.

A esto se le agrega el mantenimiento continuo, como la gestión de parches, que también se debe realizar de forma remota. El departamento de TI debe planificar el mantenimiento necesario de forma proactiva y automatizarlo siempre que sea posible.

La automatización de las tareas de rutina puede ayudar a resolver el desafío actual de la sobrecarga del personal de TI. Al programar las tareas manuales, el equipo de TI puede dar mantenimiento a varios dispositivos a la vez y ganar tiempo para enfocarse en otras tareas importantes.

Ideando una solución

Para resolver estos desafíos ineludibles, se necesita una estrategia sólida. Las empresas deben contar con un plan que ofrezca flexibilidad a los empleados cuando se trata de trabajo remoto e híbrido, al tiempo que se maximiza la seguridad en términos de privacidad y datos para poder proteger a la empresa contra los delincuentes cibernéticos que siempre están presentes.

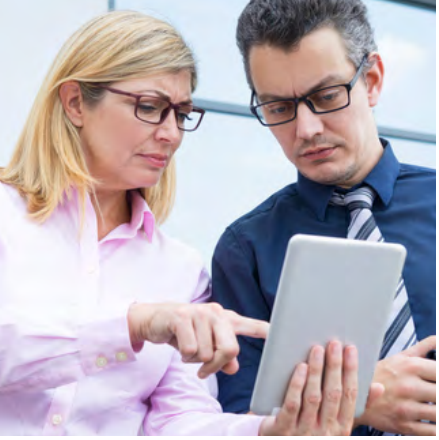
Las empresas deben contar con un plan que les ofreca flexibilidad a los empleados cuando se trata de trabajo remoto e híbrido.

Las empresas deben desarrollar una estrategia de teletrabajo y utilizar herramientas que los ayuden a lograr lo siguiente:

1. **Lograr mayor visibilidad en su entorno de TI.** Las empresas deben contar con total visibilidad para poder resolver los problemas de TI. El equipo de TI debe saber en todo momento qué empleados están utilizando aplicaciones y sistemas determinados y tomar el control del entorno de TI.
2. **Mejorar la previsión con una planificación proactiva.** Los gerentes de TI pueden prever y planear con antelación estableciendo verificaciones que envían alertas cuando sea necesario tomar acción. Un sistema de verificación bien organizado puede ayudar a los equipos de TI a solucionar los problemas más leves antes de que se vuelvan graves y causen más inconvenientes.
3. **Conectarse fácilmente a los dispositivos remotos.** Para asegurar la continuidad del negocio y ofrecerles a los empleados una asistencia constante, los equipos de TI deben conectarse fácilmente a cualquier dispositivo remoto que utilicen los empleados. Las mejores herramientas también ofrecerán asistencia remota más allá de la pantalla de las computadoras a través de la realidad aumentada (RA) para solucionar los problemas de hardware.
4. **Centralizar la gestión de parches informáticos.** Los equipos de TI pueden protegerse contra las vulnerabilidades informáticas centralizando las actualizaciones y asegurándose de que los dispositivos estén siempre al día.
5. **Automatizar las tareas siempre que sea posible.** Al automatizar las tareas rutinarias y programar las tareas que antes eran manuales, el equipo de TI les puede dar mantenimiento a varios dispositivos a la vez y ganar tiempo para enfocarse en tareas más prioritarias.
6. **Reevaluar la estrategia de protección cibernética.** Analiza si tu estrategia está a la altura de los desafíos actuales. Un personal remoto requiere una malla de ciberseguridad y también una solución que lo proteja contra los ataques de día cero.

Los beneficios de una sola solución integrada

Las empresas necesitan socios estables y seguros que los ayuden a superar todos estos desafíos. TeamViewer te ofrece un acceso remoto seguro y estable, control remoto y



Las soluciones de TeamViewer eliminan la desconexión entre lo que ven los agentes de asistencia técnica y lo que ve el usuario.

asistencia remota para casi todas las plataformas móviles y de escritorio, incluidas las PC remotas, los smartphones, los servidores, las terminales de pago y los dispositivos del IoT, en cualquier momento y en cualquier lugar.

Con el acceso y la asistencia remotos de TeamViewer, los empleados pueden acceder de forma segura a los dispositivos remotos y controlarlos como si estuvieran sentados frente a ellos, sin necesidad de una VPN. La herramienta también permite compartir archivos de forma segura y flexible.

TeamViewer Remote Management permite que el departamento de TI vea fácilmente los dispositivos de los empleados que se encuentran en cualquier parte del mundo para ofrecerles asistencia remota e instantánea cuando ocurre un fallo en un dispositivo, una computadora o en el sistema. También ofrece Patch Management para mantener actualizado el sistema operativo de cada dispositivo, así como Endpoint Protection de última generación, que protege contra las ciberamenazas (incluidos los ataques de día cero) y está completamente integrado en el entorno de TeamViewer.

El uso de TeamViewer Assist AR, una herramienta de asistencia visual que utiliza la realidad aumentada, facilita la identificación y la resolución de problemas. Sus características incluyen las siguientes:

- **Fácil visibilidad.** Durante la asistencia, los empleados pueden utilizar su teléfono para permitir que un miembro del equipo de TI lo ayude a resolver el problema en tiempo real.
- **Herramientas interactivas.** Las herramientas interactivas eliminan las dudas y la necesidad de describir verbalmente las acciones que los usuarios deben realizar para resolver un problema. Los equipos de TI pueden utilizar la realidad aumentada para dibujar en los videos de asistencia en tiempo real con punteros, flechas, círculos y texto, indicándoles a los empleados exactamente lo que hay que hacer para que no haya confusión. Al señalar y dibujar en la pantalla, los problemas se pueden solucionar de forma rápida y eficiente. Aunque el teléfono se mueva, se caiga o se deje apartado, la indicación del miembro del equipo de TI seguirá estando presente cuando se vuelva a tomar el dispositivo.

Las soluciones de TeamViewer eliminan la desconexión entre lo que ven los agentes de asistencia técnica y lo que ve el usuario y también aumentan la productividad de los empleados. Incluso, reducen los costos y los retrasos al disminuir las visitas en el lugar y de escritorio, lo que se traduce en menos viajes y menos tiempo de inactividad. Las herramientas aseguran la continuidad del negocio y les permite a las empresas ser proactivas frente a los problemas, planificar su tiempo y reaccionar al instante.

TeamViewer ayuda a las pequeñas y grandes empresas a enfrentarse a los desafíos de los entornos de TI ampliados de un mundo laboral híbrido. Las pequeñas empresas pueden utilizar los productos TeamViewer Remote Access y Assist AR, mientras que una gran empresa puede utilizar los productos TeamViewer Tensor o Frontline.

En el nuevo mundo de los lugares de trabajo remotos e híbridos actuales, las empresas no pueden sobrevivir sin una solución sólida y eficiente para gestionar y proteger el creciente número de lugares y dispositivos de trabajo. Las empresas que tendrán éxito son aquellas que le dan prioridad a la inversión en la tecnología adecuada para ayudar a proteger sus datos y su privacidad y que les ofrecen a los empleados la flexibilidad buscada.

Contacta a un experto de TeamViewer hoy mismo y descubre cómo una sola solución puede hacer toda la diferencia.