

## **Qualtic presenta medidas de ciberseguridad para proteger a los empleados en situación de teletrabajo**

**Una rápida transición al trabajo remoto ha hecho que los técnicos informáticos tengan que estar mucho más vigilantes que con el trabajo habitual en las oficinas**

Muchas empresas, preocupadas todavía por la situación sanitaria actual alterada por la pandemia de la Covid-19, continúan animando a sus trabajadores a trabajar desde casa. El cambio también podría exponer estas organizaciones a los ciberataques si no se toman precauciones.

Empresas que van desde gigantes tecnológicos hasta startups y pymes continúan apostando por el teletrabajo. Sin ir muy lejos, en la ciudad de Sant Cugat del Vallès, el teletrabajo es una tendencia que en esta segunda oleada ha marcado un 46,7% de la actividad en combinación con la jornada en el centro de trabajo. Microsoft, Alphabet, Facebook y Apple siguen instando a los empleados a trabajar desde casa, si sus tareas diarias lo permiten. Varias empresas tecnológicas, incluidas Google y Cisco, mantienen su oferta de herramientas de colaboración de forma gratuita, puesto que empresas de todo el mundo han implementado políticas de trabajo desde casa y se mantienen canceladas las conferencias físicas.

"Hemos notado cómo el trabajo a distancia no solo respondía a una necesidad del momento sino que ha venido para quedarse", afirma Marc Granados, CEO y Responsable TIC de Qualtic, empresa de soluciones informáticas personalizadas, en referencia a cómo este nuevo nivel de flexibilidad del puesto de trabajo pone a prueba la estrategia en ciberseguridad de las empresas.

La experiencia y el trabajo diario de Granados va alineada a las últimas noticias de ataques informáticos y opina que estas prácticas crecerán: "Cuando los trabajadores empiezan a conectarse desde cafeterías o espacios públicos, pueden poner en riesgo información sensible sin saberlo; aquellos que visitan otros espacios de trabajo para cambiar el paisaje pueden dejar sus dispositivos desatendidos", argumenta.

Aspectos a tener en cuenta con el teletrabajo

"En casa hay una tendencia a bajar la guardia puesto que la gente se siente más segura, de forma que cualquier mal hábito de seguridad informática desde casa se puede traducir en posibles vías de entrada para los ciberdelincuentes", explica Granados al tratar como el reto más grande es recordar y reforzar positivamente estos buenos hábitos de seguridad a partir de la formación, puesto que los propios usuarios son un punto débil que los atacantes aprovechan.

"Es posible que los empleados que trabajen desde casa no tengan las mismas herramientas de protección que en el trabajo. Por eso es clave tener una buena estrategia en seguridad y unos protocolos muy definidos", añade el CEO de Qualtic.

Los empleados también pueden perder sus credenciales o compartirlas accidentalmente a través de una Wi-Fi pública. Si un atacante los captura e inicia sesión en una aplicación empresarial, será difícil para los equipos de seguridad determinar cuál ha sido el acceso inadecuado.

#### Medidas para proteger a los empleados en situación de teletrabajo

"Se tiene que ser más proactivo en materia de prevención. Por eso es muy importante que todos los equipos y dispositivos estén actualizados con las últimas versiones disponibles", señala Granados, que aconseja a los departamentos de TI que generen materiales de formación diseñados porque los trabajadores sepan qué hacer y que pueden esperar si experimenten un incidente de seguridad. Si lo hacen, los empleados tendrían que saber informar inmediatamente sobre cualquier amenaza y preocupación que puedan tener para la seguridad.

Otro aspecto que menciona es la autenticación multifactor, basada en una confirmación del código de seguridad del usuario con el teléfono u otros dispositivos, para los usuarios que accedan a servicios empresariales sensibles a través de la red, como soluciones de acceso remoto.

Desde Qualtic resaltan que las empresas que se estén adaptando al trabajo remoto tendrían que seguir de estrategias de comunicación interna para poder estar sobre aviso de cualquier incidencia de manera rápida y efectiva. En esta línea es imprescindible poder ofrecer un buen ritmo de formaciones a los trabajadores para que puedan reconocer las amenazas que pueden tener a sus correos o teléfonos móviles. "Además de la tecnología, las personas son realmente importantes y son la primera línea de defensa que más se tiene que cuidar", puntualiza el Responsable TIC de la empresa.

#### Sobre Qualtic

Son especialistas en asesoramiento tecnológico y disponen de todo tipo de servicios y soluciones para adaptarlas a las necesidades de los clientes más exigentes. En la actualidad dan soporte a todo tipo de clientes: pequeñas o medianas empresas y administraciones públicas.

#### Datos de contacto:

EDEON MARKETING SL

Comunicación · Diseño · Marketing

931929647

Nota de prensa publicada en: [Barcelona](#)

Categorías: [Programación](#) [Hardware](#) [E-Commerce](#) [Software](#) [Ciberseguridad](#) [Dispositivos móviles](#) [Oficinas](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>