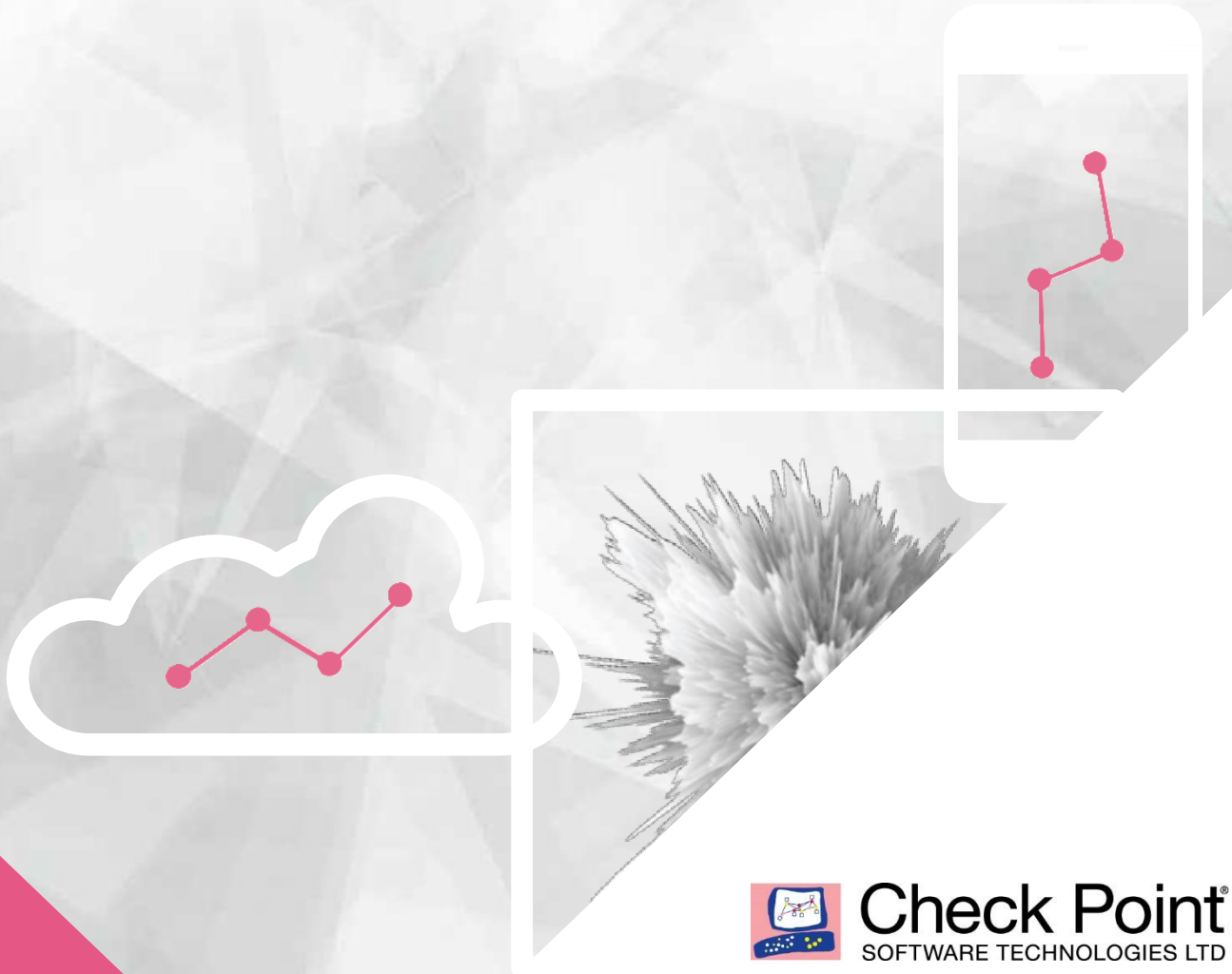
# Ciberseguridad en el Teletrabajo para la continuidad del negocio en tiempos del Coronavirus. Retos y Recomendaciones



Check Point
SOFTWARE TECHNOLOGIES LTD

# Los mejores consejos para un trabajo remoto seguro

**Consejos prácticos para permitir a los empleados trabajar de forma segura desde su hogar durante el brote de coronavirus.**

¿Estamos frente a una pandemia sin precedentes, o nuestros temores serán infundados? Es imposible decirlo en este momento, pero las preocupaciones globales sobre la propagación actual del coronavirus y lo que sucederá después con el brote están impulsando a las compañías a revisar cómo sus empleados realizan sus tareas diarias.

Millones de personas en toda Asia han comenzado a trabajar desde casa . Las principales compañías tecnológicas como Amazon, Microsoft, Facebook y otras grandes empresas han pedido a su fuerza laboral que trabajen de forma remota hasta que la situación mejore y el virus esté contenido. A la luz de todo esto, empresas como JP Morgan han tomado medidas para probar sus políticas e infraestructura de trabajo remoto. En España el Gobierno facilita el Teletrabajo tras anunciar el cierre de colegios y universidades de la Comunidad de Madrid y Vitoria. Este inminente cambio de paradigma de trabajo significa que cada miembro de la fuerza laboral debe prepararse para el día en que se les indique que trabajen desde casa.

Trabajar desde casa no es complicado. La mayoría de nosotros lo hacemos de vez en cuando. Acceder a una conexión a Internet es bastante fácil, y las suites de ofimática en la nube y las aplicaciones SaaS facilitan la transición de trabajar en la oficina a hacerlo en el sofá de la sala de estar. Pero la mayoría de las organizaciones no habrán preparado a tantos empleados para trabajar de manera remota, y los propios empleados pueden no conocer las mejores prácticas de seguridad cuando trabajan desde casa.

Así que definitivamente es el momento de revisar y mejorar la seguridad en torno al acceso remoto a datos corporativos, en ambos extremos de la conexión. Estos son nuestros mejores consejos para trabajar de forma remota y segura para los empleados y las empresas.

# Mejores prácticas para empleados

Naturalmente, tendemos a estar más relajados en casa, especialmente cuando se trata de seguridad. Después de todo, nos sentimos cómodos con la seguridad de nuestros propios hogares, entonces, ¿Qué podría salir mal? Desafortunadamente, los ciberdelincuentes están tratando de explotar exactamente este tipo de situaciones con ataques y amenazas de phishing cuidadosamente diseñadas. Puntos a tener en cuenta por los empleados:

- **Las contraseñas son importantes**: es una buena idea revisar y fortalecer las contraseñas que utiliza para iniciar sesión en recursos remotos, como correo electrónico o aplicaciones de trabajo.
- **Tenga cuidado** con la **suplantación de identidad (phishing)**: tenga cuidado de hacer clic en los enlaces que parecen sospechosos y solo descargue contenido de fuentes confiables que

puedan verificarse. Recuerde que las campañas de phishing son una forma de ingeniería social, por lo que, si recibe un correo electrónico con una solicitud inusual, verifique cuidadosamente los detalles del remitente para asegurarse de que se está comunicando con colegas, no con delincuentes. Nuestro equipo de investigación descubrió que los dominios relacionados con Coronavirus tienen un 50% más de probabilidades de ser maliciosos , así que asegúrese de echar un ojo sobre cualquier cosa inesperada que aparezca en su buzón.

- **Elija su dispositivo con cuidado**: muchos empleados usan el PC o portátil de su empresa para uso personal, lo que puede crear un riesgo de seguridad. El riesgo es aún mayor si utiliza un portátil personal para fines laborales. Si tiene que usar un portátil personal para el trabajo, hable con su equipo de TI sobre cómo fortalecer la seguridad, por ejemplo, agregando un paquete de seguridad endpoint y antivirus.
- **¿Quién está escuchando?** ¿La red wifi de su hogar tiene una contraseña segura o está abierta? Asegúrese de que esté protegido contra cualquier persona dentro del alcance que pueda acceder y conectarse a la red. Lo mismo se aplica al trabajo desde una cafetería u hotel: tenga cuidado al conectarse a redes inalámbricas públicas. Las redes no seguras facilitan el acceso de los ciberdelincuentes a correos electrónicos y contraseñas.

# Mejores prácticas para las empresas

Esta guía debería servir como punto de partida para las organizaciones, ya sea para que sus aplicaciones y datos estén almacenados en centros de datos, nubes públicas o dentro de aplicaciones SaaS.

- **No confíes en nadie**: todo tu plan de acceso remoto debe construirse utilizando la mentalidad de cero confianza/Zero Trust, donde todo debe verificarse y no debe suponerse nada. Asegúrese de comprender quién tiene acceso a qué información, segmentando a sus usuarios y asegurándose de autenticarlos con una autenticación multifactor. Además, ahora es el momento de reeducar a sus equipos para que entiendan por qué y cómo acceder a la información de manera segura y remota.
- **Cada endpoint necesita atención**: en un escenario típico, es posible que haya personas trabajando en escritorios dentro de la oficina. Suponiendo que sus dispositivos no van a casa con ellos, ahora existirán una gran cantidad de dispositivos desconocidos que necesitan acceso a sus datos corporativos. Debe pensar con anticipación sobre cómo manejar las amenazas planteadas por la fuga de datos, los ataques que se propagan desde el dispositivo a su red, y debe asegurarse de que la postura de seguridad general de los dispositivos sea suficiente.
- **Haga una prueba de resistencia de su infraestructura**: para incorporar herramientas seguras de acceso remoto en sus flujos de trabajo, es fundamental tener una VPN o un SDP. Esta infraestructura debe ser robusta y debe someterse a prueba de esfuerzo/stress para garantizar que pueda manejar un gran volumen de tráfico, a medida que su fuerza laboral cambia el rumbo para trabajar desde su casa.
- **Defina sus datos**: Tómese el tiempo para identificar, especificar y etiquetar sus datos confidenciales, a fin de prepararse para políticas que aseguren que solo las personas apropiadas puedan acceder a ellos. No haga suposiciones sobre la gestión de datos anterior y adopte un enfoque granular que le servirá una vez que el acceso remoto esté

completamente habilitado. Nadie quiere proporcionar accidentalmente a toda la organización acceso a recursos humanos.

- **Segmente su fuerza de trabajo**: ejecute una auditoría de sus políticas actuales relacionadas con el acceso y el intercambio de diferentes tipos de datos. Vuelva a evaluar tanto la política corporativa como su segmentación de los equipos dentro de su organización, para que pueda estar seguro de que tiene diferentes niveles de acceso que se correlacionan con los diversos niveles de sensibilidad de datos.

Estas piedras angulares de la seguridad de acceso remoto ayudarán a las organizaciones a proteger mejor sus datos y redes contra amenazas e intercepciones en ambos extremos de la conexión.

## Contacte con nosotros. Asegure sus equipos remotos hoy.

Sede en España | Vía de las Dos Castillas, 33, 28224 Pozuelo de Alarcón (Madrid) | Tel: 91 799 27 14 | Fax: 650-654-4233
Email: info_iberia@checkpoint.com / www.checkpoint.com/es