GUÍA DE TRABAJO REMOTO PARA PYMES

Manual de teletrabajo seguro para administradores IT

El trabajo a distancia es esencial para la continuidad de una empresa durante el caos social de estos días. Sin embargo, si se introduce de manera apresurada para mantener a los empleados productivos y el negocio en marcha, puede suponer una brecha en la seguridad de tu empresa. Y si por algo destacan los cibercriminales, es por no desaprovechar las oportunidades que se les brinda. Por ello, sigue esta lista paso a paso y podrás proteger tu empresa independientemente desde donde estéis trabajando.

☐ Refuerza tu política de contraseñas

Fortalece las medidas de seguridad relacionadas con las contraseñas. Permite únicamente la utilización de contraseñas largas (mejor si además contienen símbolos), obliga a cambiarlas cada poco tiempo y bloquea las cuentas después de un determinado número de fallos de acceso. Explícales también a tus empleados que no deben utilizar las mismas contraseñas que usan en sus cuentas personales.

☐ Utiliza un doble factor de autenticación

La autentificación multifactor es tu mejor defensa contra los cibercriminales que usan ataques de fuerza bruta, robo de contraseñas o compra de credenciales en la dark web para hacerse pasar por empleados e infiltrarse en tu red. Si utilizas un servidor de correo, un paquete de programas o aplicaciones en la nube, un doble factor de autentición es tu solución. Establécela también en caso de que tus empleados necesiten acceder a la red interna de la empresa.

☐ No permitas el acceso a la red interna de la empresa sin una VPN

Una VPN encripta el tráfico al navegar por Internet para que nadie externo a tu empresa pueda acceder a la información. Además, la conexión por VPN permite al personal de sistemas aplicar más medidas de seguridad en los equipos conectados a distancia. En caso de que algunos de tus trabajadores ya estén conectados a la VPN, asegúrate de que tienes licencias suficientes para el resto. Asimismo, utilizar tanto la VPN como un doble factor de autenticación es fundamental si tus empleados tienen que acceder a datos o información de la red de la empresa.

☐ A ser posible, utiliza una solución de escritorio virtualizado

Con esta solución, el empleado puede acceder a una máquina virtual que se encuentra en la nube o en tu centro de datos y controlarla a distancia. Se puede configurar para que se parezca al sistema de una oficina. La ventaja es que la información delicada se guarda en la máquina y no en el equipo del trabajador.

☐ Recomienda a tus empleados que utilicen redes seguras

No puedes controlar la red personal de un empleado ni los dispositivos que se conectan a esta. Por ello, tienes que explicarles que deben deshabilitar cualquier carpeta compartida en el sistema que vayan a utilizar para trabajar y comprobar que sus puntos de acceso WiFi tengan el WPA2 activado. Recuérdales que nunca se conecten a una red WiFi pública o desprotegida.

Asegúrate de que los ordenadores de tus empleados estén totalmente protegidos

El antivirus preinstalado en el ordenador desde el que teletrabaja tu empleado puede no estar a la altura. Una solución de seguridad completa debe proteger contra todo tipo de amenazas con múltiples capas de defensa, incluido un cortafuegos personal, protección contra páginas web fraudulentas y malware alojado en USBs. La mejor opción en este caso sería utilizar una protección avanzada que tu personal de sistemas pueda administrar de forma remota.

Implementa la encriptación de datos si tus empleados trabajan con información confidencial

En caso de que tus empleados se tengan que descargar información de la empresa en sus equipos privados, facilítales un método de encriptación. Recuérdales que separen los archivos privados de los laborales y que guarden estos últimos en una carpeta encriptada. Asimismo, aconséjales que guarden los documentos en el almacén de datos de la empresa para que no tengas que preocuparte por la copia de seguridad a distancia.

Fomenta el hábito de cerrar sesión

Los empleados que estén más de uno o dos minutos sin utilizar sus ordenadores, ya sea porque es la hora de comer o porque han finalizado la jornada laboral, deben cerrar la sesión en la red de la empresa. Es bueno hacerlo siempre, sobre todo si se comparte el equipo u otras personas tienen acceso a él.

Promueve los parches y actualizaciones

Recomienda a los empleados que trabajan desde casa que habiliten las actualizaciones automáticas en sus sistemas operativos para que dispongan de las últimas medidas de seguridad. Comprueba varias veces que tus sistemas también están actualizados, sobre todo aquellos que consideres vitales para la seguridad debido a su continuo funcionamiento. Ten especial cuidado con los ordenadores que utilicen todavía Windows 7, pues este ya no dispone de actualizaciones. Es más, tal vez convendría bloquear el acceso de estos equipos hasta que cuenten con un sistema operativo con soporte.

Facilita información sobre ciberseguridad a tus empleados

No importa de cuánta tecnología dispongas, un actor clave en la protección son los empleados. Falsos avisos del trabajo para confirmar las credenciales de acceso, visitas a páginas web relacionadas con la empresa, solicitudes del jefe para facilitar un pago o transferencia de fondos y otras estafas irán en aumento mientras los ciberdelincuentes traten de aprovecharse de los empleados que están teletrabajando. Los empleados conocedores de estos engaños son menos propensos a caer en ellos. Información o formación en ciberseguridad de manera regular los ayudará a estar más protegidos.

Buenas noticias

Las plataformas en la nube, la colaboración online a través de chats y vídeoconferencias y otros métodos de comunicación online pueden ayudar a que los que trabajan desde casa sean tan productivos como cuando están en la oficina, a veces incluso más. Solamente debes asegurarte de que estén correctamente ciberprotegidos.

Para más información acerca de las soluciones de ESET, visita nuestra página web