

ACCESO REMOTO SEGURO

Es posible que los empleados y proveedores necesiten conectarse a su red de manera remota.

Ponga la seguridad de su red en primer lugar. Exíjales a todos que sigan sólidos estándares de seguridad antes de conectarse a su red. Ofrézcales las herramientas para que incorporen la seguridad a su rutina de trabajo.

CÓMO PROTEGER LOS DISPOSITIVOS

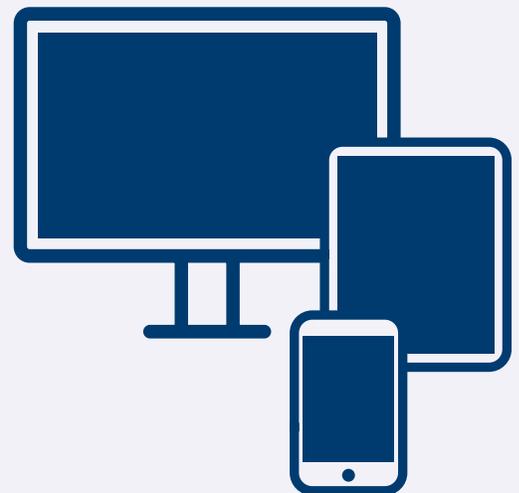
Cuando los empleados o proveedores se conectan de manera remota a su red, ya sea a través de los dispositivos de propiedad de su compañía o de sus propios dispositivos, esos dispositivos deben estar protegidos. Siga estas recomendaciones – y asegúrese de que sus empleados y proveedores también lo hagan:

Cambie la contraseña preestablecida y el nombre predeterminado de su enrutador. Y mantenga actualizado el programa del enrutador; es posible que para hacerlo tenga que visitar a menudo el sitio web del enrutador.

Considere activar la codificación completa de los discos de las computadoras portátiles y otros dispositivos móviles que se conectan a su red de manera remota. Busque esta opción en su sistema operativo que protegerá todos los datos almacenados en el dispositivo en caso de robo o pérdida. Esto es especialmente importante si en el dispositivo se almacena información personal delicada.

Cambie la configuración de los teléfonos inteligentes para impedir las conexiones automáticas a las redes Wi-Fi de uso público.

Mantenga actualizado el programa antivirus en los dispositivos que se conectan a su red, incluidos los dispositivos móviles.



CÓMO CONECTARSE REMOTAMENTE A LA RED

Exíjales a los empleados y proveedores que usen conexiones seguras cuando se conecten a su red de manera remota. Ellos deberían:

Usar un enrutador con una codificación de tipo WPA2 o WPA3 cuando se conecten desde sus casas. La codificación protege la información que se envía a través de una red para que las personas ajenas a su negocio no puedan leerla. Los sistemas de codificación WPA2 y WPA3 son los únicos estándares de codificación que protegerán la información enviada a través de una red.



Usar únicamente una red Wi-Fi pública cuando también estén usando una red virtual privada (VPN, por sus siglas en inglés) para codificar el tráfico entre sus computadoras e internet. Las redes Wi-Fi de uso público no ofrecen una conexión segura a internet por sí solas. Sus empleados pueden obtener un VPN, o tal vez le convenga crear una red virtual privada empresarial para que la usen todos sus empleados.

QUÉ TIENE QUE HACER PARA MANTENER LA SEGURIDAD

Capacite a su personal:

Incluya información sobre acceso remoto seguro en las sesiones regulares de capacitación y en las reuniones de orientación para el personal nuevo.

Establezca políticas que cubran los conceptos básicos de ciberseguridad, entrégueles copias a sus empleados y explique la importancia de cumplir dichas políticas.

Antes de permitir la conexión de cualquier dispositivo a su red — ya sea desde la casa de un empleado o desde la red de un proveedor — asegúrese de que el usuario cumpla con los requisitos de seguridad de su red.

Informe a su personal acerca del riesgo que presentan las redes Wi-Fi de uso público.



Ofrézcales a los miembros de su personal las herramientas que los ayudarán a mantener la seguridad:

- Exíjales a los empleados que usen contraseñas únicas y complejas para la red y que eviten que los puestos de trabajo abiertos queden al descuido.
- Exija una autenticación de múltiples factores para acceder a las áreas de su red que contengan información delicada. Esto requiere algunos pasos adicionales además de iniciar la sesión con una contraseña — como un código temporario enviado a un teléfono inteligente o una llave que se inserta en una computadora y genera un código.
- Considere crear una red VPN para los empleados conectarse a la red del negocio de manera remota.
- Si en su negocio ofrece una red Wi-Fi para visitantes y clientes, asegúrese de que esté separada y no conectada a la red de su negocio.
- Incluya disposiciones de seguridad en sus contratos con los proveedores, especialmente si el proveedor se conectará a su red de manera remota.