GUÍA DE TRABAJO REMOTO PARA LAS PYME

Guía de acceso remoto seguro: checklist para administradores de TI

Cuando ocurre una interrupción social, es esencial habilitar una opción de trabajo desde el hogar para no perder la continuidad del negocio. Sin embargo, en el esfuerzo por mantener a los trabajadores productivos y el negocio funcionando, aplicar una opción de trabajo remoto en forma precipitada puede dejar a su organización vulnerable en términos de seguridad. Siga los pasos detallados en la siguiente lista de verificación para proteger a los trabajadores sin importar cuál sea su ubicación.

- [ ] **Ajuste sus políticas de uso de contraseñas**
  Exija el uso de contraseñas largas, solicite que se cambien en forma periódica y bloquee las cuentas tras un número determinado de ingresos erróneos. Explique a los empleados que no pueden volver a utilizar sus contraseñas laborales en ninguno de sus inicios de sesión personales.

- [ ] **Use la autenticación en varias fases (MFA)**
  La MFA constituye su mejor defensa contra los ciberdelincuentes que emplean técnicas de ataque de diccionario con contraseñas robadas o compradas en la Dark Web para hacerse pasar por empleados e infiltrarse en su red. Si usa correo electrónico o aplicaciones basadas en la nube, active la función de MFA. Si los usuarios necesitan acceder a su red interna, instale una solución con MFA.

- [ ] **Utilice una VPN para acceder a su red interna**
  Una VPN cifra el tráfico corporativo cuando atraviesa la Internet pública para que no pueda ser leído por terceros. Además, una conexión VPN le permite a su equipo de TI aplicar más medidas de seguridad de su red interna a los dispositivos remotos. Si ya está utilizando una VPN para algunos empleados, asegúrese de contar con suficientes licencias y capacidad para poder proteger a los nuevos usuarios. Si los empleados van a acceder a los recursos en su red interna, es imprescindible usar una combinación de VPN y MFA.

- [ ] **Utilice una interfaz de escritorio virtual**
  Con este tipo de solución, el empleado accede a una máquina virtual que se encuentra en la nube o en su centro de datos, y la controla de manera remota. La máquina virtual se puede configurar para que se vea exactamente como el sistema que usa en la oficina. La ventaja es que los datos o archivos confidenciales solo existen en la máquina virtual y nunca se almacenan en el sistema doméstico del empleado.

- [ ] **Resalte la responsabilidad al utilizar la red y las conexiones de Wi-Fi**
  Pídale a sus colaboradores que desactiven el uso compartido de archivos en el sistema que usarán para trabajar, y que verifiquen que la seguridad WPA2 de su router doméstico o punto de acceso Wi-Fi esté habilitada. Recuérdeles que nunca se conecten a una red Wi-Fi no segura o abierta.

- [ ] **Implemente una solución de seguridad que permita proteger el trabajo remoto**
  Una solución completa que reúna todas las funcionalidades protegerá el sistema ante todo tipo de amenazas gracias a sus múltiples capas de defensa, que incluyen un firewall personal, protección contra sitios Web maliciosos y protección contra malware en unidades USB portátiles. En este caso, la mejor opción es adquirir una suite de seguridad para endpoints de nivel corporativo que su departamento de TI pueda administrar en forma remota.

- [ ] **Utilice el cifrado para trabajar con archivos confidenciales**
  Además, insista a sus colaboradores en que mantengan sus archivos personales separados de los documentos corporativos y que guarden dichos documentos en una carpeta cifrada. Además, aplique una política para que guarden los documentos utilizados en el almacén de datos de la empresa; de esa forma, no deberá preocuparse por hacer un backup remoto.

- [ ] **Inculque el hábito de cerrar la sesión**
  Cuando los colaboradores se toman un descanso o dejan el dispositivo fuera de su alcance por más de un minuto deben cerrar la sesión en la red corporativa. Resulta particularmente imprescindible si la computadora se comparte o si otras personas de la casa pueden acceder a ella.

- [ ] **Incentive la instalación de parches y actualizaciones**
  Pídale a los colaboradores que habiliten las actualizaciones automáticas en todos sus sistemas. Verifique que su entorno interno también esté actualizado, en especial los elementos y sistemas críticos para la seguridad que funcionan 24x7 y podrían tener parches pendientes de instalación. Preste atención a las máquinas hogareñas con Windows 7: limite el acceso hasta actualizarlas con una versión más reciente.

- [ ] **Capacite a sus colaboradores en seguridad IT**
  Los supuestos mensajes de la empresa para confirmar las credenciales de inicio de sesión, la visita de sitios Web relacionados con el trabajo, el pedido del jefe para realizar un pago o transferencia de fondos y muchas otras estafas serán cada vez más comunes a medida que los ladrones cibernéticos se las vayan ingeniando para llegar a los trabajadores conectados desde sus hogares. Los empleados bien informados y alertas tienen menos probabilidades de caer en la trampa. Especialmente cuando trabajan de manera remota, un programa de capacitaciones periódicas hará que no bajen la guardia.

Y ahora las buenas noticias

Las herramientas de trabajo en la nube, la colaboración online mediante chat y conferencias, y otras tecnologías conectadas a Internet y de acceso remoto pueden lograr que los trabajadores sean tan productivos desde sus hogares como en la oficina. **Asegúrese de suministrarles las medidas de seguridad correctas.**

Más información sobre nuestras soluciones: www.eset.com/latam