




Cómo lograr que su plantilla remota esté preparada para la cibernética

Aunque la tecnología permite a las personas trabajar de forma remota, también abre la puerta a nuevos riesgos para la ciberseguridad y la protección de datos.


Ahora más que nunca, cada organización necesita contar con un responsable de preparación cibernética designado, alguien que guíe a su plantilla. Para obtener más información sobre nuestro Programa de preparación cibernética gratuito y la función del responsable cibernético visite nuestro sitio web (www.cyberreadinessinstitute.org).

Estas son las tres áreas fundamentales que los directores deben tener en cuenta a la hora de establecer una plantilla preparada para la cibernética:




-  ¿Qué dispositivos usarán las personas para conectarse y acceder a la información?
-  ¿Cómo se conectarán para acceder a la información?
-  ¿Cómo accederán, gestionarán y protegerán la información?

Dispositivos

Si los empleados usan un dispositivo facilitado por la empresa desde casa:

-  Recuerde a los empleados que cumplan las políticas de contraseña/frase de contraseña y actualización de software


Si los empleados usan dispositivos personales:


-  Que tengan diferentes contraseñas/frases de contraseña para uso personal y laboral
-  Que instalen y ejecuten un software de detección de virus
-  Que actualicen todo el software antes de conectarse a la red de su organización

-  Que activen las actualizaciones automáticas para todo el software


-  Que activen la autenticación multifactor siempre que se ofrezca

Si los empleados usan dispositivos personales compartidos (con su cónyuge, hijos, etc.):


-  Que cierren y salgan de todas las aplicaciones al final de cada sesión de trabajo

-  Que acaben la sesión, cierren y salgan de las bases de datos o navegadores web

-  Que no escriban las contraseñas/frases de contraseña y las dejen en el ordenador o cerca de él.


-  Que no almacenen contraseñas/frases de contraseña en el dispositivo ni usen el inicio de sesión automático


Si los empleados usan ordenadores públicos (por ejemplo, en un parque, bibliotecas, cafés, etc., si están abiertos):

-  Este uso se debe desaconsejar encarecidamente y solo se debe hacer si es esencial.

-  Que cierren y vuelvan a abrir las aplicaciones que ya estaban abiertas

-  Que usen la navegación privada en el navegador web si es posible

-  Que cierren y salgan de todas las aplicaciones, incluidos los navegadores web, al final de cada sesión de trabajo

-  Que no guarden nunca ningún documento en el ordenador público

-  Si usan una unidad USB, lo cual no es recomendable, que no la inserten nunca en un ordenador público



Conexiones

Si los empleados usan una conexión Wi-Fi personal desde su domicilio:

- Que cambien la contraseña/frase de contraseña del Wi-Fi existente antes de comenzar a trabajar de forma remota

Si los empleados usan un hotspot personal o facilitado por la empresa

- Que usen siempre el hotspot en lugar de la red Wi-Fi pública

Si los empleados usan una red Wi-Fi pública:

- En general, los empleados deben evitar el uso del Wi-Fi público salvo que su organización tenga una red privada virtual (VPN) que los empleados sepan cómo utilizar



Gestión del acceso y los datos

Enumere a qué sistemas y datos puede acceder cada empleado en las operaciones normales.

¿Será necesario realizar algún cambio en lo que pueden acceder cuando trabajan de forma remota?

En cuanto al uso de dispositivos USB, es mejor prohibirlos y proporcionar un intercambio de archivos basado en la nube para transferir, compartir y almacenar datos:

- Si su organización tiene una política de “no usar dispositivos USB”, recuérdese a los empleados y recalque lo importante que es cumplir la política mientras se trabaja de forma remota
- Si su organización permite el uso de dispositivos USB (no es una buena idea), proporcione a cada empleado uno que haya sido analizado en busca de malware. Indique a los empleados que solo pueden utilizarlo en el ordenador que usarán para trabajar de forma remota Y que se aseguren de que tienen un software de detección de virus en el ordenador ANTES de insertar el dispositivo USB

Compartir y guardar el trabajo de los trabajadores remotos puede plantear nuevos retos.

- Si su organización ha estado usando el intercambio de archivos centralizado (OneDrive, Google Drive, i-Cloud, Box, Drop Box, etc.), los empleados estarán acostumbrados a gestionar el modo en que colaboran para trabajar en documentos



Si no es así, debe establecer unas pautas sobre el modo en que los empleados gestionan y comparten los documentos:

De modo ideal, debería preparar un sitio para compartir archivos.

Mientras tanto, indique a los empleados que envíen los documentos como archivos adjuntos de correo electrónico cifrados. Muchas aplicaciones de correo electrónico (Outlook, Gmail, Apple Mail, etc.) permiten cifrar los archivos adjuntos. Existen programas complementarios que ofrecen cifrado para correos electrónicos y archivos adjuntos (Virtu, Tutanota, VMware Boxer, Symantec Desktop, etc.)

Sus directrices deberían incluir la denominación de documentos y algunos conceptos básicos del control de versiones. Si los empleados guardan documentos de trabajo en un dispositivo personal, necesita un método para evitar tener varias versiones del mismo documento.



Nos comprometemos a ser un recurso fundamental para ayudar a las pymes a compaginar el trabajo remoto y la ciberseguridad. No dude en ponerse en contacto con nosotros si tiene preguntas, comentarios o casos de éxito (support@cyberreadinessinstitute.org).

Acerca del Cyber Readiness Institute

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de seguridad cibernética gratuitas para las pequeñas y medianas empresas (pymes). El Programa de preparación cibernética autodirigido y en línea se encuentra disponible en chino, inglés, francés, español, portugués, árabe y japonés.

Para obtener más información, visite www.becyberready.com.