CYBER READINESS
INSTITUTE

Preparación cibernética para el lugar de trabajo híbrido: **políticas que las personas seguirán**

Empresas de todos los tamaños reconocen ahora que va a haber una “nueva realidad” más permanente en el lugar de trabajo. Muchas empresas solo envían un pequeño porcentaje de su personal a la oficina física, lo que significa que el entorno de trabajo híbrido —algunos empleados trabajan desde casa y otros desde la oficina— se convertirá en una realidad.

Esta realidad requiere que las empresas desarrollen e implementen políticas de ciberseguridad resilientes que aborden el lugar de trabajo híbrido. Durante los primeros meses de la pandemia, muchas empresas tuvieron que centrarse en la continuidad del negocio y relajaron las políticas de seguridad para ayudar a las personas a trabajar con eficacia desde ubicaciones remotas. Ahora ha llegado el momento de sustituir esas políticas de seguridad relajadas por el desarrollo de políticas híbridas que garanticen la misma seguridad en todos los entornos de trabajo.

El CRI se centra en ayudar a las pequeñas y medianas empresas (pymes) a establecer políticas y procedimientos seguros en este entorno híbrido.

Tanto para los directores como para los empleados, tiene sentido pensar en la preparación cibernética del lugar de trabajo híbrido en términos de Personas, Procesos y Tecnología. Aunque puede que algunos de ustedes hayáis utilizado bastante estas categorías, ofrecen una forma útil de pensar y comunicar la preparación cibernética, especialmente a las personas que tratan de comprender cómo abordar los problemas de ciberseguridad en este entorno dinámico.

Personas: ¿qué cambios de comportamiento son necesarios para ser productivos y estar preparados para la cibernética?

Proceso: ¿qué cambios en las políticas y los procedimientos son necesarios para definir expectativas claras para el comportamiento de los empleados y prepararlos para triunfar?

Tecnología: ¿qué nueva tecnología es necesaria para mejorar la ciberseguridad cuando los empleados trabajan de forma remota o cambian habitualmente entre el hogar y la oficina?

guide@cyberreadinessinstitute.com

El Cyber Readiness Institute se centra en el comportamiento humano —las personas y los procesos del marco descrito anteriormente— pero también brindaremos orientación sobre tecnología en el entorno de trabajo híbrido.

A continuación, se incluyen consejos importantes para ayudar a los directores a dar prioridad a lo que deben hacer para garantizar un entorno híbrido.

Asegúrese de que todos los empleados estén formados y se sientan cómodos con las políticas de su organización sobre:

- **Contraseñas:** una autenticación fuerte incluye el uso de frases de contraseña de más de 16 caracteres y de autenticación de múltiples factores, siempre que sea posible.
- **Phishing:** brinde formación frecuente y actualizada sobre actividades de phishing en la que incluyan ejemplos de intentos recientes de phishing en el hogar o en el trabajo, especialmente en relación con la COVID-19.
- **Utilización del USB:** proporcione directrices disciplinadas acerca de cómo trabajar en los documentos de la empresa desde múltiples ubicaciones. Este enfoque podría incluir formación y la implantación de un sistema de intercambio de archivos basado en la nube.
- **Actualizaciones de software:** describa las expectativas de que las actualizaciones se descarguen de inmediato en cualquier dispositivo que se utilice para acceder a la red de la empresa.

Todas las empresas deben intentar entregar un ordenador portátil de trabajo a todos los empleados que trabajan desde casa para evitar el uso de dispositivos personales para trabajar. Si esto no es posible desde el punto de vista financiero, trabaje con sus empleados para configurar una cuenta de usuario independiente en su dispositivo personal.

Dada la creciente dependencia de las plataformas de comunicaciones por vídeo, asegúrese de utilizar plataformas con protocolos de seguridad, incluido el uso de una contraseña distinta para cada reunión.

Establezca comunicaciones proactivas y periódicas con su equipo, entre las que se incluyan:

- Llamadas semanales al personal
- Controles individuales programados con regularidad

Permanezca atento a las guías adicionales de nuestra serie sobre el lugar de trabajo híbrido, ya que desmitificamos la ciberseguridad en esta nueva realidad y entorno de trabajo al ofrecer consejos para directores y empleados.

Acerca del CRI

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 ciberseguridad gratuitas para las pequeñas y medianas empresas (pymes). Nuestros recursos de trabajo remoto están disponibles en español y francés. El Programa de Preparación Cibernética autodirigido y disponible en línea se encuentra en chino, inglés, francés, español, portugués, árabe y japonés. Para obtener más información, visite www.BeCyberReady.com.