CYBER READINESS
INSTITUTE

Conceptos básicos de protección de datos para trabajadores remotos

Como respuesta a la pandemia de la COVID-19, se produjo un rápido cambio al trabajo remoto. Ahora, a medida que la pandemia entra en una nueva fase, estamos viendo otro cambio hacia un entorno de trabajo híbrido, en el que algunos empleados trabajarán desde casa, otros desde la oficina y otros tanto desde el hogar como desde la oficina. Esta nueva realidad probablemente se prolongará al menos durante todo el año y planteará nuevos desafíos en la protección de datos.

La protección de los datos de su organización es importante para la seguridad y sostenibilidad de su empresa y usted, como empleado, desempeña un papel fundamental en dicha protección. Si todas las personas están concienciadas, la organización puede crear una cultura de preparación cibernética que se extienda desde el hogar hasta la oficina.

Para muchos trabajadores remotos, los datos a los que accederán son documentos (procesamiento de texto, hojas de cálculo, o presentaciones), archivos (contabilidad) o bases de datos (gestión de clientes o seguimiento de pedidos). El activo más importante de su empresa son los datos y una sólida ciberseguridad los protege. Para cumplir las reglas básicas de protección de datos, probablemente deberá cambiar ciertos aspectos de su comportamiento.

Para empezar, tenga siempre en cuenta qué dispositivo (por ejemplo, teléfono, portátil) está utilizando (de la empresa o personal), cómo se conecta a Internet (por ejemplo, WiFi doméstico, cafetería, biblioteca) y la red de su empresa (por ejemplo, si usa una VPN o no) y cómo accede, transfiere, almacena y trabaja con los datos (por ejemplo, correo electrónico, aplicaciones, etc.).

guide@cyberreadinessinstitute.com

Estos son los consejos fundamentales de protección de datos para trabajar de forma remota y/o en un entorno híbrido remoto/de oficina. Hemos agrupado los consejos en algunas categorías básicas:

Acceso a los datos

- No comparta nunca sus contraseñas ni credenciales de inicio de sesión
- Sepa qué información se considera confidencial y con quién se puede compartir

Almacenamiento y uso de los datos

- Sepa dónde almacena sus documentos: servidor de la empresa, almacenamiento en la nube, almacenamiento en la nube personal, ordenador personal, medios extraíbles (USB)
- Si usa un ordenador compartido, no almacene nunca información confidencial en él
- Marque la información confidencial con un nombre apropiado (por ejemplo, confidencial, patentada)
- Asegúrese de que la información confidencial esté protegida en su domicilio de la misma forma que lo hace en el trabajo.
- Use los procedimientos de control de versiones y denominación de documentos de su empresa; si no hay ninguno, añada un número de versión a los nombres de los documentos (por ejemplo, Anuncio_de_nuevo_producto_V1.docx se convertiría en Anuncio_de_nuevo_producto_V2.docx)
- Debe evitar guardar documentos en su ordenador personal para trabajar en ellos

Compartir datos

- No comparta nunca documentos sensibles (es decir, confidenciales, patentados) sin aprobación, incluso con compañeros de su organización
- Use cifrado siempre que sea posible; si es absolutamente necesario enviar información confidencial como un archivo adjunto, asegúrese de que el documento esté cifrado o protegido con contraseña

Busque más consejos y herramientas del Cyber Readiness Institute (CRI) en las próximas semanas. Nos comprometemos a ser un recurso fundamental para ayudar a las pequeñas y medianas empresas (pymes) a crear culturas de ciberseguridad, de forma remota y en la oficina. Para acceder a guías adicionales sobre preparación cibernética para los trabajadores remotos, visite

WWW.CYBERREADINESSINSTITUTE.ORG/REMOTE-WORK-RESOURCES

Para obtener más información sobre nuestro Programa de preparación cibernética gratuito y cómo convertirse en un responsable cibernético y acceder a guías adicionales sobre preparación cibernética para los trabajadores remotos, visite **becyberready.com**

CYBER READINESS
INSTITUTE

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**.

guide@cyberreadinessinstitute.com