CYBER READINESS
INSTITUTE

¿Debo recurrir a asistencia externa para gestionar mis riesgos de ciberseguridad?

Esta es la primera parte de una serie de cinco entregas sobre el uso de empresas externas para reducir sus riesgos en cuanto a ciberseguridad.

Si usted es como la mayoría de los propietarios o directores de pequeñas empresas, tiene muchas funciones. Su atención suele centrarse en los elementos fundamentales de la gestión y el desarrollo de su negocio. Sabe que la ciberseguridad es un área de riesgo en crecimiento porque ha habido más noticias al respecto, especialmente sobre amenazas y ataques cibernéticos. La ciberseguridad es multifacética. Es cierto que los firewalls y los filtros antispam ayudan, pero también necesita un personal bien formado que conozca los elementos básicos de la ciberseguridad. El Cyber Readiness Institute se centra en el comportamiento humano y la educación para crear una cultura de seguridad dentro de cada organización. Al fin y al cabo, basta con un clic erróneo en un enlace de phishing para arruinar potencialmente su negocio. Si esto suena abrumador, lo adecuado es buscar orientación. Esta serie de cinco entregas del Cyber Readiness Institute, en consulta con su Consejo Asesor de Pymes, le guiará por el proceso de determinar si necesita ayuda externa y, en caso afirmativo, cómo obtenerla.

Quizás solía pensar que no sería un objetivo de los piratas informáticos, pero ahora está claro que están atacando a las pequeñas empresas para obtener beneficios financieros, como mediante la instalación de ransomware, y utilizándolas como puertas de enlace para atacar a empresas más grandes. Sabe que debe hacer algo, pero no está seguro de lo qué o si necesita ayuda externa. **Recuerde, puede externalizar algunas de sus responsabilidades en materia de ciberseguridad, pero no puede subcontratar su responsabilidad en este ámbito.** Con o sin ayuda externa, siempre será su responsabilidad crear y fomentar una cultura de preparación cibernética dentro de su organización.

info@cyberreadinessinstitute.com

El primer paso es analizar honestamente su riesgo en cuanto a ciberseguridad. Dé prioridad a los sistemas y los datos que necesita para dirigir su empresa. A continuación, se ofrecen algunos consejos rápidos para empezar:

1. Enumerar **la información y los datos más importantes** para el éxito de su organización (por ejemplo, la información del cliente, la información comercial confidencial).
2. Enumerar las **herramientas de hardware y software informático que son más importantes** para el funcionamiento de su organización (por ejemplo, sitio web, correo electrónico, almacenamiento de archivos, sistema de contabilidad, bases de datos).
3. De las listas anteriores, identificar los tres o cinco elementos más importantes que causarían el mayor daño a su organización si no estuvieran disponibles, se perdieran o fueran robados. A estos les llamaremos las **joyas de la corona**.
4. Identificar quién tiene **acceso a sus joyas de la corona**. Determinar de manera realista lo bien protegidos que están y si se siente cómodo con el **nivel de protección**.
5. Si no puede saber lo bien protegidas que están, tiene que buscar apoyo externo.
6. Si necesitan una mejor protección, ¿sabe qué hacer y puede conseguirlo? Si no es así, necesita ayuda externa.
7. Determine si existen requisitos de protección de datos, ciberseguridad o privacidad de datos por parte de sus clientes o leyes y normativas federales o locales aplicables.

CYBER READINESS
INSTITUTE

No se preocupe si parece que debe considerar la posibilidad de obtener ayuda externa. La mayoría de las pequeñas empresas necesitan asistencia externa para TI y ciberseguridad. Como organización sin ánimo de lucro, estamos aquí para brindar asesoramiento gratuito y sencillo. Podemos ayudarle a comprender la diferencia entre un consultor de TI, un proveedor de servicios gestionados (MSP) y un proveedor de servicios de seguridad gestionados (MSSP). Podemos brindarle orientación sobre dónde y cómo utilizar los servicios en la nube para ayudar a su empresa a ser más cibersegura y resiliente.

Hubo un tiempo en que la ciberseguridad no se consideraba un elemento “fundamental” de la gestión de una empresa; ese tiempo ya ha pasado. Debe centrarse en ella del mismo modo que prioriza sus finanzas, las relaciones con los clientes y los recursos humanos. De los últimos años de ciberataques y violaciones, hemos aprendido que no debe esperar a que ocurra un desastre para prestar atención a la ciberseguridad.

Vuelva pronto para ver las próximas guías de la serie o **regístrese aquí** para recibir una notificación por correo electrónico cuando se publiquen.

Al evaluar su riesgo en cuanto a ciberseguridad, piense en la pérdida de datos y la continuidad del negocio.

Si es una empresa de contabilidad, por ejemplo, perder los datos de los clientes es probablemente mucho peor que tener su sitio web caído durante una semana. Si vende productos y servicios en línea, que su sitio web se caiga durante una semana podría ser extremadamente perjudicial.

Lista completa de las guías de esta serie:

¿Debo recurrir a asistencia externa para gestionar mis riesgos de ciberseguridad?
(ESTA GUÍA)

Introducción a los tipos de asistencia externa de TI y ciberseguridad

Cómo seleccionar el nivel idóneo de asistencia externa

Revisión y comprensión del contrato

Sus responsabilidades continuas en materia de ciberseguridad

Autores colaboradores

Agradecimientos especiales

- **Marc Pillon**, IT Ally
- **Jennifer Khoury**, NCMS
- **Pam Hurt**, NCMS
- **Brian Kelly**, EDUCAUSE
- **Dawn Yankeelov**, TALK
- **Lee Ann Lyle**, TALK
- **Faye Francy,** Auto-ISAC
- **Ilene Klein**, Cybercrime Support Network
- **Jill Tokuda**, CyberHawaii
- **John Bryk**, DNG-ISAC
- **Michael Pritchard**, Netchex
- **Tanya Bolden**, AIAG
- **Walter Bran**, ICC Guatemala
- **Stan Stahl**, SecureTheVillage
- **Lisa McAuley**, GTPA
- **Kiersten Todt**, CRI
- **Chris Caine**, CRI
- **Craig Moss**, CRI
- **Marion Lewis**, CRI
- **Lessie Longstreet**, CRI
- **Ira Sager**, CRI
- **Monica Consiglio**, CRI
- **Vivek Ghelani**, CRI

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). Explore los elementos básicos de una buena ciberseguridad con nuestro Kit básico o cree una cultura de preparación cibernética en su organización con el Programa de Preparación Cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite www.BeCyberReady.com.