CYBER READINESS
INSTITUTE

Introducción a empresas externas que ofrecen asistencia de TI y ciberseguridad

Segunda entrega de una serie sobre el uso de empresas externas para reducir su riesgo en cuanto a ciberseguridad.

Como muchas pequeñas empresas, ha llegado a la conclusión de que necesita asistencia externa de tecnología de la información (TI) y ciberseguridad. Tal vez haya oído más noticias de violaciones de ciberseguridad. Quizás conozca una empresa que ha sufrido un ataque de ransomware. Si aún no está seguro de si necesita ayuda, eche un vistazo a la **primera guía** de esta serie, "¿Debería obtener asistencia externa para gestionar mi riesgo en cuanto a ciberseguridad?"

Es consciente de que la TI y la ciberseguridad se están convirtiendo en "elementos fundamentales" de la gestión empresarial, como las finanzas y las ventas. Pero no tiene tiempo para resolverlo todo. Si usted es como la mayoría de los propietarios o directores de pequeñas empresas, puede que no esté seguro de qué tipo de asistencia necesita o incluso de qué preguntas plantear. Esta serie del Consejo Asesor de pymes del Cyber Readiness Institute le guiará a través del proceso para determinar si necesita asistencia externa y cómo obtener la ayuda que necesita.

Recuerde siempre que, en última instancia, es responsable de la preparación cibernética de su organización. Puede externalizar ciertas funciones, como la instalación de actualizaciones de software, pero es responsable de establecer las políticas, crear una cultura cibernética y cumplir con las obligaciones de cumplimiento de seguridad y privacidad.

A medida que ha ido aumentando la amenaza de los ciberataques, también lo ha hecho el número y los tipos de empresas que ofrecen su asistencia. Se trata de un mercado complicado con ofertas de servicios que se solapan y más siglas de las que pueda imaginar.

info@cyberreadinessinstitute.com

Una de las primeras decisiones que debe tomar es si desea contratar a un asesor informático/cibernético de confianza que le guíe a través del proceso o explorar los distintos proveedores por su cuenta. Sabemos que la idea de contratar a un consultor para elegir al proveedor o a los proveedores adecuados puede parecer un gasto adicional. Sin embargo, a largo plazo puede ser más rentable, porque le puede garantizar que obtendrá los servicios que necesita a un precio justo. En última instancia, debe determinar en quién confiar para obtener la ayuda que necesita.

A continuación, se ofrece una lista de los **tipos de empresas** que encontrará y una breve descripción. Recuerde que habrá cierta superposición en los tipos de servicios que prestan. En la siguiente guía de la serie trataremos cómo seleccionar el nivel adecuado de asistencia externa.

Consultor de TI

Similar a un técnico de TI. En términos generales, el consultor de TI ayuda a evitar que se produzcan problemas y los soluciona cuando surgen. Ayuda a configurar su red y/o WiFi, crear y mantener sitios web, recomendar e instalar software, configurar correos electrónicos, configurar cuentas de usuario, crear y probar copias de seguridad, etc.

Proveedor de servicios gestionados (MSP)

Los MSP (por sus siglas en inglés, Managed Service Provider) suelen ser pequeñas empresas que ofrecen servicios similares a los consultores de TI. Con frecuencia son instaladores certificados o asesores de varios proveedores de hardware y software. Algunos MSP afirman que están especializados en ciberseguridad, lo que significa que sus servicios se superpondrán en mayor medida con los de un MSSP.

Proveedor de servicios de seguridad gestionados (MSSP)

El MSSP (por sus siglas en inglés, Managed Security Services Provider) verificará que el MSP esté creando y manteniendo la red para maximizar el valor y reducir el riesgo, ya que algunos MSP y consultores de TI tienen un conocimiento limitado sobre supervisión o tecnología de ciberseguridad. Los MSSP a menudo realizan actividades como mapeo de intrusiones, verificación de registros, evaluación de riesgos tecnológicos, planificación y consultoría, cumplimiento de políticas, desarrollo de procedimientos, asistencia al usuario, respuesta de seguridad proactiva, supervisión y respuesta ante incidentes.

Responsable de información virtual (vCIO)

Para las empresas que pueden necesitar un CIO en su plantilla, los vCIO (por sus siglas en inglés, Virtual Chief Information Officer) ofrecen una forma de subcontratar la función, similar a subcontratar las funciones de un asesor jurídico o un director financiero. Este concepto tiende a ser para empresas que son un poco más grandes dentro de las pymes. Los vCIO administrarán, implementarán y recomendarán productos y servicios para mejorar sus niveles de seguridad y TI.

info@cyberreadinessinstitute.com

A continuación se ofrece una lista de **los tipos de certificaciones más habituales y respetadas** o las credenciales profesionales que puede encontrar al evaluar a los proveedores de asistencia externa.

Credenciales generales de ciberseguridad:

CISSP (Certified Information Systems Security Professional) - Profesional certificado en seguridad de sistemas de información

- Se trata de una certificación general pero avanzada, con una amplia aplicación, ya que no es específica de un proveedor. Se requieren 5 años de experiencia para obtenerla.

CISM (Certified Information Security Manager) - Responsable de seguridad de la información certificado

- Se trata de una certificación avanzada que requiere cinco años de experiencia para obtenerla. Las personas que obtienen esta credencial por lo general administran la seguridad a nivel organizativo (por ejemplo, CISO).

CompTIA Security+

- Una certificación básica que proporciona una buena base para obtener otras credenciales más avanzadas.

Credenciales especializadas (según la necesidad):

SANS

- SANS ofrece una variedad de certificaciones técnicas, divididas en áreas de enfoque como seguridad en la nube, pruebas de penetración y piratería ética, gestión de seguridad, legal y auditoría.
- La certificación SANS GIAC Security Essentials (GSEC) plantea un equilibrio óptimo e indica que el titular de esta credencial posee una base de conocimiento aplicable de forma amplia, así como habilidades técnicas específicas.

CISA (Certified Information Security Auditor) - Auditor certificado en seguridad de la información

- Como indica el nombre, esta credencial está indicada para funciones centradas en auditoría y cumplimiento.

CIPP (Certified Information Privacy Professional) - Profesional certificado en privacidad de la información

- Esta credencial se centra en la privacidad de los datos en lo que respecta a cuestiones legales y normativas.

CEH (Certified Ethical Hacker) - Hacker ético certificado

- Esta credencial significa que la persona ha aprendido a pensar como un pirata informático, pero usa esas habilidades para proteger y evitar ataques, en lugar de acceder a un sistema con intenciones malignas.

Esta guía proporciona información sobre los tipos de organizaciones y credenciales que puede encontrar. Si ahora se pregunta cómo seleccionar el tipo correcto de asistencia externa para su empresa, consulte la siguiente guía de esta serie, **“Cómo seleccionar el nivel idóneo de asistencia externa”.**

info@cyberreadinessinstitute.com

Lista completa de las guías de esta serie:

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

Introducción a los tipos de asistencia externa de TI y ciberseguridad

(ESTA GUÍA)

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
- Brian Kelly, EDUCAUSE
- Dawn Yankeelov, 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

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.

info@cyberreadinessinstitute.com