CYBER READINESS
INSTITUTE

Cómo seleccionar el nivel idóneo de asistencia externa

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

Si está leyendo esta guía, probablemente haya leído nuestra **primera guía** de esta serie, "¿Debería obtener asistencia externa para gestionar mi riesgo en cuanto a ciberseguridad?" y haya decidido que sí debería buscar algún tipo de asistencia externa. Su siguiente pregunta posiblemente habrá sido: ¿cuáles son las distintas opciones en lo que respecta a asistencia externa? Para responder a eso, consulte nuestra **segunda guía** en esta serie, "Introducción a empresas externas que ofrecen asistencia de TI y ciberseguridad".

Ahora que comprende sus opciones, está listo para descubrir cómo seleccionar la mejor para sus necesidades concretas. En esta guía, ofrecemos instrucciones paso a paso sobre cómo seleccionar el nivel idóneo de asistencia externa. Le recomendamos que guarde, descargue o imprima esta guía y que la use como hoja de trabajo personalizable para su empresa.

Paso 1: Priorizar

Establezca prioridades en cuanto a sus sistemas y sus datos. ¿Cuáles son los más importantes para su negocio? ¿Cuáles son las "joyas de la corona"? Enumérelas a continuación.

info@cyberreadinessinstitute.com

Paso 2: Plantearse contratar a un asesor

Hágase las siguientes preguntas sobre si recurrir a asistencia adicional es un paso lógico en el caso de su empresa.

¿Tengo que cumplir con normativas?

Sí **No**

¿Interactúo con información de los empleados, información identificable personalmente (IIP) de los clientes o información médica protegida (IMP)?

Sí **No**

¿Mi empresa está situada en un Estado que aplica leyes de privacidad?

Sí **No**

¿Estoy completamente informado de los requisitos y las expectativas que tienen mis clientes?

Sí **No**

¿Acepto tarjetas de crédito como forma de pago?

Sí **No**

¿Formo parte de una cadena de suministro de infraestructura esencial?

Sí **No**

Si las respuestas a las preguntas anteriores son en su mayoría “sí”, entonces probablemente le resulte útil contar con un asesor sobre seguridad de la información/asesor de ciberseguridad/ responsable virtual de seguridad de la información (vCISO, por sus siglas en inglés, Virtual Chief Information Security Officer). Pueden ofrecerle ayuda adicional para guiarle a través del proceso de selección de asistencia externa.

Si ha respondido “no” a la mayoría de preguntas anteriores, es posible que no necesite ayuda externa para determinar qué servicios externos necesita. Si este es el caso, le recomendamos que realice el Programa de preparación cibernética y el Programa de certificación de líder cibernético y que posteriormente vuelva a evaluar sus necesidades.

Paso 3: Distinguir diferentes funciones

Hay cientos de empresas y personas dispuestas a brindarle asistencia externa. Saber identificar a la mejor empresa externa para abordar sus necesidades comerciales supone un desafío. Puede que muchos consultores no tengan la formación y la experiencia adecuadas que se necesitan para responder a sus requisitos de seguridad únicos.

Para obtener más información sobre los tipos de organizaciones de asistencia, las credenciales profesionales que indican que una persona posee los conocimientos necesarios y los tipos de organizaciones que puede encontrar, vuelva a consultar la **segunda guía** en esta serie: “Introducción a los tipos de asistencia externa de TI y ciberseguridad”.

Proveedor de servicios gestionados (MSP)

El coste de los MSP (por sus siglas en inglés, Managed Service Provider) puede oscilar entre 75 y 200 dólares estadounidenses por hora. Algunos cobran una tarifa plana en lugar de una tarifa por hora y otros cobran en función de la cantidad de ordenadores o de personas.

CISO virtual (vCISO)

La cantidad de tiempo necesario y las tarifas varían, pero el coste de contratar a un vCISO podría ser de alrededor de cientos de dólares a la semana.

Paso 4: Seleccionar un responsable cibernético

El responsable cibernético crea una cultura de seguridad y garantiza que las protecciones relacionadas se implementan con la ayuda de la alta dirección y del vCISO. El responsable cibernético es la persona de contacto en su empresa entre el MSP y el vCISO, si ha contratado a un vCISO.

Paso 5: Determinar sus requisitos

La siguiente tabla enumera algunos de los requisitos y de las acciones más habituales con los que puede necesitar ayuda. Al distinguir entre MSP y vCISO, use las casillas de verificación a continuación para indicar qué elementos son relevantes para su empresa.

Si tiene problemas para comprender los términos y conceptos en la columna de la derecha, consulte a su MSP o plantéese contratar a un asesor para obtener ayuda.

MSP

- [ ] Configuración de una red en un centro
- [ ] Configuración de una red en una oficina
- [ ] Configuración de una red remota
- [ ] Configuración de ordenadores para nuevos usuarios
- [ ] Configuración de cuentas de correo electrónico
- [ ] Instalación y mantenimiento de software de respuesta y detección de endpoints (antivirus)
- [ ] Realización de copias de seguridad de datos
- [ ] Realización de pruebas de las copias de seguridad
- [ ] Establecimiento de autenticación multifactor
- [ ] Configuración de una VPN
- [ ] Instalación y mantenimiento/actualización de software
- [ ] Definición/implementación de servicios en la nube
- [ ] Prestación de servicios de asistencia
- [ ] Implementación de firewalls basados en la arquitectura de su red
- [ ] Determinación de las normativas de privacidad de datos relevantes (por ejemplo, RGPD, ley CCPA)

vCISO (Asesor de seguridad de la información)

- [ ] Evaluación/comparación de ofertas de MSP
- [ ] Creación de un plan de respuesta ante incidentes
- [ ] Supervisión del acceso, el firewall y otros registros y respuesta ante anomalías
- [ ] Seguimiento de intentos de ataque
- [ ] Realización de pruebas de penetración en la red
- [ ] Establecimiento de un uso aceptable de dispositivos personales
- [ ] Establecimiento de contraseñas y otros estándares
- [ ] Verificación de que los sistemas se actualicen de forma rápida y adecuada
- [ ] Definición de requisitos y especificaciones técnicas, como VPN, firewall, otras protecciones de seguridad (controles), arquitectura de red y/o servicios en la nube
- [ ] Realización de una revisión de riesgos de proveedores
- [ ] Garantía de que no se pueda acceder a los ordenadores desde fuera de la red
- [ ] Apoyo a la dirección de la empresa en la configuración de la cultura
- [ ] Definición de las implicaciones de seguridad de los proveedores de servicios en la nube, establecimiento de estándares
- [ ] Definición e implementación de métodos para controlar el acceso a sistemas e información para que los usuarios autorizados tengan acceso a lo que necesiten y no más
- [ ] Alineación de controles para cumplir con las normativas relevantes de privacidad de datos

Si ha marcado la mayoría de las casillas de la columna de la izquierda, debe contratar a un MSP. Si ha marcado la mayoría de las casillas de la columna de la derecha, debe contratar a un vCISO.

Si ha marcado más o menos el mismo número de casillas en ambos lados, plantéese contratar a ambos.

La finalidad de esta guía es ayudarle a determinar cómo seleccionar el nivel correcto de asistencia. Si ahora se enfrenta a contratos confusos, consulte nuestra próxima guía de esta serie, “Revisión y comprensión del contrato”.

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

Cómo seleccionar el nivel idóneo de asistencia externa

(ESTA GUÍA)

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.