CYBER READINESS
INSTITUTE

# Comprensión de su contrato de proveedor de ciberseguridad

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

En este punto del proceso, ha decidido solicitar ayuda externa para mejorar su ciberseguridad. Le ofrecemos orientación sobre los distintos tipos de proveedores de servicios y algunos consejos sobre cómo evaluarlos. En esta guía, facilitamos información sobre lo que usted (y/o su abogado) deberían buscar en el contrato. Aparte de sus aspectos legales, el contrato es un documento fundamental para definir exactamente qué servicios se prestarán y sus responsabilidades continuas en materia de ciberseguridad.

Le sugerimos que use el contrato como una lista de verificación para asegurarse de que usted y su proveedor de servicios tienen un conocimiento mutuo de las responsabilidades futuras. Querrá asegurarse de que se cumplan todas sus expectativas. No caiga en la trampa de esperar a que se produzca un incumplimiento para entender qué cubre un contrato y darse cuenta de que no cubre lo que necesita.

Es importante desarrollar una relación de confianza con su proveedor de servicios. De modo ideal, el proveedor se convertirá en parte del equipo que ayudará a su organización a crear y mantener una capacidad informática funcional y segura. Asegurarse de que entiende el contrato y las responsabilidades del proveedor es fundamental para establecer la confianza desde el principio. Además, le sugerimos que realice una auditoría trimestral con el proveedor de servicios durante la cual utilice el contrato como una lista de verificación para evaluar la relación y cómo atiende a su empresa y sus necesidades. Las amenazas a la ciberseguridad evolucionan rápidamente y querrá asegurarse de que usted y su proveedor de servicios no solo respondan, sino que implementen medidas de modo proactivo para estar protegidos y ser resilientes.

Hemos dividido esta guía en tres partes: **Revisión previa al contrato, lista de verificación del contrato y orientación sobre la revisión del contrato.**


info@cyberreadinessinstitute.com

## Revisión previa al contrato

Antes de entrar en un análisis detallado del contrato, es importante saber las prioridades, los antecedentes y la experiencia de su posible proveedor. Estos son algunos aspectos fundamentales sobre el proveedor propuesto que debe analizar ANTES de firmar el contrato. No hay respuestas “correctas” a las siguientes preguntas; tienen como objetivo ayudarlo a entender el nivel de sofisticación de su proveedor.

### Preguntas para su proveedor

1. Identifique su(s) punto(s) de contacto con el proveedor para servicios específicos y quién será su gerente de relaciones de modo continuo.
2. Verifique que los empleados del proveedor han pasado las comprobaciones de seguridad adecuadas (es decir, comprobaciones de antecedentes) para gestionar la información patentada.
3. Confirme que su proveedor tiene un seguro cibernético y verifique el alcance/límite de la cobertura en caso de un incidente cibernético en su empresa. Esto servirá para identificar las posibles brechas de la cobertura entre el seguro del proveedor y el seguro que puede que usted tenga o no.
4. Pregunte sobre su nivel de controles de seguridad y si se ajustan a algunas normas o marcos (certificaciones o credenciales como NIST 800-53, NIST Cybersecurity Framework, ISO27001, FedRamp y/o informes de auditoría, como un SOC2).
5. Sepa las horas de soporte del servicio (es decir, ¿es el horario comercial habitual o las 24 horas del día, los 7 días de la semana?) ¿Cuál es la disponibilidad del proveedor “fuera del horario”?
6. Si aloja software o datos, sepa dónde está alojado y quién controla esos servidores y solicite a los proveedores que le notifiquen cualquier cambio. En algunos casos, es posible que el proveedor solo le ofrezca soporte y no aloje ninguno de sus datos o software.
7. Determine si el proveedor está usando otros servicios de otras compañías o subcontratistas para ofrecerle el servicio.
8. Pregunte si el proveedor forma parte de alguna organización o servicio que ofrezca inteligencia sobre amenazas.

## Lista de verificación del contrato

A continuación, ofrecemos algunas pautas para evaluar el contrato que tiene con su proveedor de ciberseguridad. En la tabla siguiente, damos algunas sugerencias sobre los servicios obligatorios que deben especificarse en el contrato, junto con algunos elementos opcionales que debe tener en cuenta.

## Obligatorio

- ☐ Disponibilidad del servicio de asistencia: horas de soporte disponibles incluidas en el paquete de precios básico
- ☐ Documentación y guías de usuario del hardware y software correspondientes
- ☐ Configuración del hardware (es decir, servidores, portátiles, Wi-Fi, smartphones)
- ☐ Instalación y actualizaciones de software
- ☐ Soporte técnico de red
- ☐ Asesoría (CIO virtual)
- ☐ Copia de seguridad y recuperación (alcance, pruebas y frecuencia)
  - **¿Las copias de seguridad se realizan fuera de línea?**
  - **¿Las copias de seguridad están cifradas?**
- ☐ Prácticas de cifrado de datos
  - **¿Se cifran los datos almacenados?**
  - **¿Se cifran los datos en tránsito?**
- ☐ Definición del nivel de respuesta prioritaria (a continuación se incluyen algunos ejemplos)
  - **PRIORIDAD 1: en toda la empresa; con impacto financiero inmediato; menos de 30 minutos**
  - **PRIORIDAD 2: problemas específicos del departamento o de la aplicación; de 30 minutos a 4 horas**
  - **PRIORIDAD 3: una persona afectada; de 4 a 8 horas**
- ☐ Cláusula de escalamiento con el proveedor para problemas no resueltos
- ☐ Contactos de respuesta ante incidentes principales (proveedor y cliente)
- ☐ Expectativas mínimas para los controles de seguridad
  - **Configuración de Active Directory o equivalente para el control de acceso**
  - **Configuración de red**
  - **Momento de las actualizaciones (por ejemplo, el proveedor aplicará parches para las vulnerabilidades críticas en 1 a 3 días hábiles)**
  - **El proveedor deberá notificar si hay una brecha de seguridad dentro del plazo establecido**
  - **Objetivo del alojamiento y tiempo de actividad que incluye un tiempo de inactividad previsto máximo**
  - **Visibilidad de dónde se alojan los datos**
  - **Proceso y horario de incorporación**
- ☐ Cláusula de terminación del cumplimiento

## Opcional

- ☐ Arquitecto/administrador de redes y sistemas
- ☐ Servicios de asesoría (no especificados en otra parte) y compartir las prácticas recomendadas del sector
- ☐ Asistencia al usuario para trabajadores remotos
- ☐ Asistencia al usuario para empleados que usan dispositivos personales
- ☐ Asistencia fuera del horario
- ☐ Capacidad de compra (descuentos en hardware y software por compras de gran volumen)
- ☐ Comprobación de registros (frecuencia)
- ☐ Frecuencia y alcance de los informes de actividad de la red
- ☐ Participación en ejercicios de respuesta cibernética, incluida la formación en simulación y respuesta a incidentes
- ☐ Formación (tipo y frecuencia, por ejemplo, autenticación multifactor, VPN, transferencia segura de datos, etc.)
- ☐ Asistencia para desarrollar un Plan de respuesta a incidentes
  - **Responsabilidad y funciones en un incidente**
  - **Costes adicionales asociados con un incidente**



info@cyberreadinessinstitute.com

## Orientación sobre la revisión del contrato

Algunos problemas son negociables, pero debe asegurarse de que sabe lo que busca en un proveedor y que ha identificado el tipo de proveedor correcto antes de suscribir un contrato formal. Si necesita ayuda para seleccionar el tipo de proveedor correcto, vuelva a leer las **guías anteriores** de esta serie.

A continuación se incluye un extracto de muestra de un contrato que describe el enfoque general de un proveedor para la relación y el servicio que ofrecerá. No todos los proveedores de servicios proporcionarán tantos detalles sobre su enfoque, pero puede usarlo como una guía para algunos de los elementos generales que se deben abordar:

> "Nuestro equipo y el Centro de soporte también se encargan de la gestión de la red y actúan como punto focal para todas las necesidades de gestión de contratos de los proveedores. **Además, ofrecemos un equipo cualificado, la infraestructura y los recursos para el diseño y desarrollo web y de software para proyectos como sitios web basados en bases de datos**. [MSP] proporciona un método proactivo y personalizado para la resolución de problemas. La misión de [MSP] incluye ofrecer un entorno profesional y centrado en el cliente para la **administración y soporte del sistema in situ** Cumplimos nuestra misión mediante la combinación adecuada de personas, procesos y tecnología. Nuestro método nos permite prestar los más altos niveles de atención al cliente, a través de nuestra plantilla in situ y de forma remota a través de nuestro Centro de soporte. **Desplegamos tecnologías de calidad y documentación personalizada con reglas de negocio específicas**, **flujos de trabajo y catálogos de planes de dispositivos/ accesorios/tarifas, para permitir una tecnología que implemente las políticas**. Otros servicios prestados: el [MSP] ofrece alternativas al soporte y la **solución de problemas de grandes estaciones de trabajo y servidores** , **dispositivos inalámbricos**, protección de la información, **cifrado de datos**, **protección preventiva del firewall**, conexiones informáticas seguras, biometría, gestión de proyectos informáticos, **centro de llamadas**, control de recursos y soporte informático, **vigilancia Web**".

En la página siguiente se incluye un extracto con disposiciones contractuales específicas. Observe el nivel de detalle del horario y el periodo de los servicios y la especificidad sobre la responsabilidad del cliente:

**ANEXO A, DECLARACIÓN DE TRABAJO N.º S1-2017-205-433**

*Sujeto a los términos del Acuerdo de servicios profesionales ("Acuerdo"), las Partes suscriben esta Declaración de trabajo ("SOW").*

## Terminación

1. Periodo de cumplimiento: el Periodo inicial de cumplimiento será del 1 de noviembre de 2018 al 30 de noviembre de 2019. Salvo que una Parte envíe un aviso por escrito de la terminación antes del final del Periodo inicial de cumplimiento, el Acuerdo continuará mes a mes hasta una Parte notifique por escrito la terminación de conformidad con el Acuerdo.

## Horario estándar del servicio de asistencia

2. Servicios: los Servicios se prestarán in situ o de forma remota, según lo determine el [MSP] a su discreción exclusiva, principalmente en la ubicación del Cliente. El soporte estándar se prestará entre las 9:00 am y las 6:00 pm hora del Este de Estados Unidos, de lunes a viernes, excepto los días festivos observados por el Cliente. Se proporcionará soporte de emergencia fuera del horario de atención y supervisión de la red las 24 horas del día, los 7 días de la semana y los 365 días del año.

## Velocidad de servicio

3. 2.1 Servicios cubiertos 2.1.1. **Servicio de asistencia:** El [MSP] proporcionará un sistema de emisión de tickets (ConnectWise) y una herramienta de **gestión de supervisión remota** (RMM) (N-able) además de un antivirus (Sophos). El Cliente enviará todos los problemas a través del portal del cliente en línea, correo electrónico o línea directa. El Cliente podrá recibir asistencia por correo electrónico, teléfono o de forma remota para ayudar a resolver cualquier problema informático que pueda retrasar la productividad. **En caso de una emergencia en el emplazamiento, un técnico del [MSP] acusará recibo en un plazo de 30 minutos y empezará a desplazarse al emplazamiento en un plazo de 2 horas.** Cualquier mantenimiento in situ que no sea de emergencia se programará entre el [MSP] y el Cliente, pero se podrá solicitar al [MSP] que se **realice en un plazo de 4 horas hábiles si el Cliente determina que es necesario para garantizar las operaciones informáticas.** El [MSP] responderá in situ en cualquier instalación del Cliente en el área de [ciudad] y el desplazamiento NO se considerará un coste adicional. El [MSP] gestionará el correo electrónico del Cliente realizando la gestión de los usuarios finales, añadiendo o eliminando cuentas de correo electrónico, perfiles de usuario y configuración de los ordenadores. El Cliente deberá avisar en el plazo de 5 días hábiles antes de la configuración o eliminación de un nuevo usuario. El Cliente rellenará la plantilla del Portal del cliente facilitada por el [MSP] para los nuevos usuarios y la supresión de usuarios".

Esta guía fue diseñada para ayudarlo a revisar y entender los posibles contratos antes de comprometerse formalmente con un proveedor. En nuestra próxima y última guía de esta serie, describiremos cómo gestionar la relación en curso una vez firmado el contrato. Recuerde, la finalidad del contrato es definir las expectativas para establecer una relación de confianza entre usted y su proveedor de servicios.

## Lista completa de las guías de esta serie:

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

Introducción a los tipos de asistencia externa de TI y ciberseguridad

Cómo seleccionar el nivel idóneo de asistencia externa

Revisión y comprensión del contrato

(ESTA GUÍA)

Sus responsabilidades continuas en materia de seguridad cibernética

## 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
- Lisa McAuley, Global Trade Professionals Alliance
- Srinath Sogal, Cyber Academy for Kids through Empowerment
- Kathy Schultz, SUNY Cobleskill
- Sean Filipowski, SUNY Cobleskill

## 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 seguridad cibernética 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.