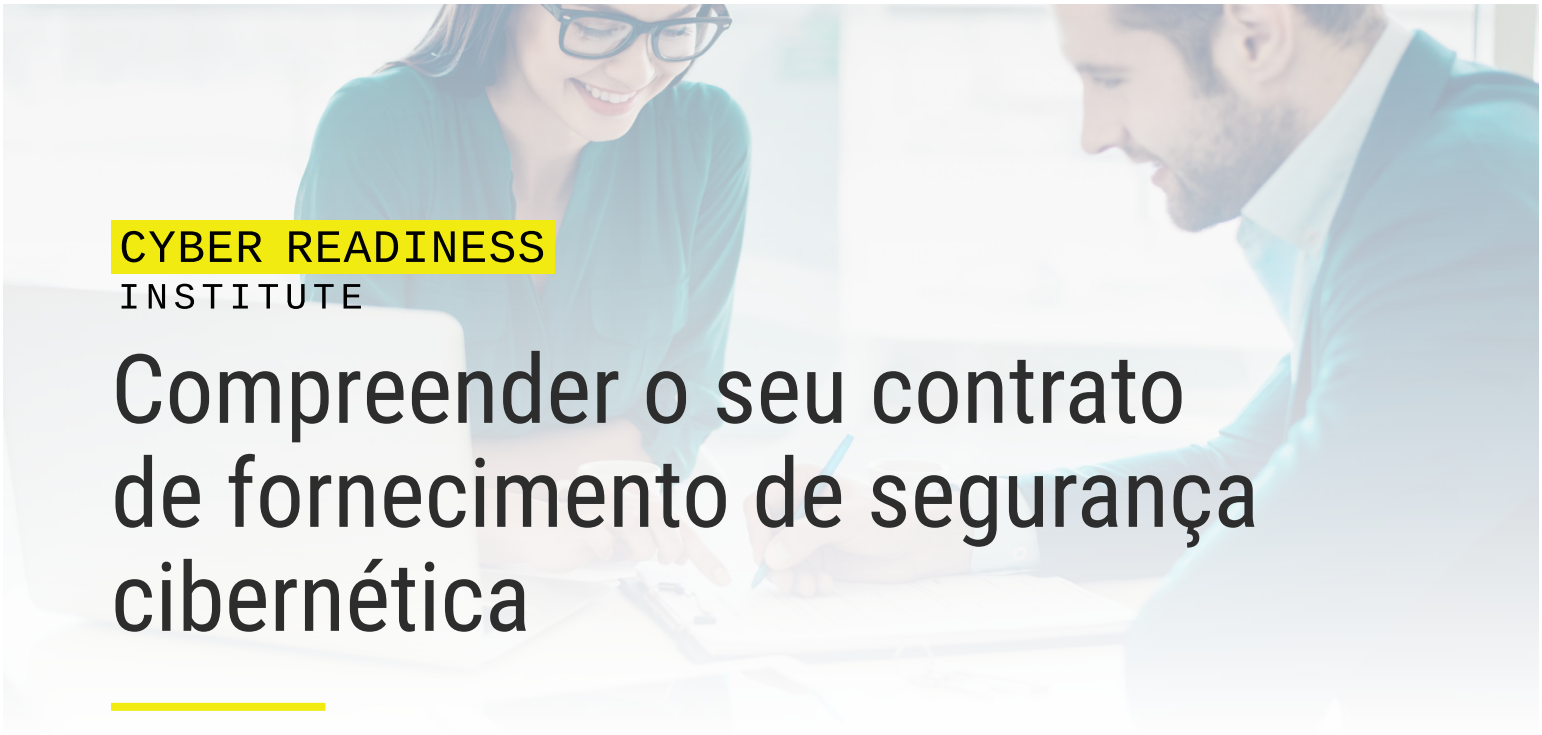

CYBER READINESS
INSTITUTE

Compreender o seu contrato de fornecimento de segurança cibernética

Este guia é o quarto guia de uma série de cinco partes sobre como utilizar empresas externas para reduzir o risco de segurança cibernética.

Nesta fase do processo, decidiu recorrer a apoio externo para melhorar a cibersegurança. Demos-lhe orientação sobre os vários tipos de prestadores de serviços e sugestões para os avaliar. Neste guia, falamos daquilo a que deve estar atento (ou o seu advogado, ou ambos) no contrato. Para além das questões legais, o contrato é um documento fundamental para definir exatamente que serviços serão prestados e as suas responsabilidades contínuas de cibersegurança.

Recomendamos que use o contrato como uma lista de verificação, para garantir que tanto você, como o seu prestador de serviços, entendem as responsabilidades daqui em diante. É importante garantir que todas as expectativas são abordadas. Não caia na armadilha de esperar até haver uma violação de segurança para saber o que o contrato cobre e aperceber-se de que não cobre as suas necessidades.

É importante desenvolver uma relação de confiança com o seu prestador de serviços. De preferência, o fornecedor fará parte da equipa que ajuda a organização a criar e manter uma capacidade funcional e segura em TI. Garantir que compreende o contrato e as responsabilidades do fornecedor é fundamental para criar confiança desde o início. Além disso, recomendamos que realize uma auditoria trimestral com o prestador de serviços. Durante a mesma, use o contrato como uma lista de verificação para avaliar a relação e se esta satisfaz a empresa e as suas necessidades. As ameaças de cibersegurança evoluem rapidamente, e é importante garantir que você e o seu prestador de serviços não se limitam a reagir, mas implementam proativamente medidas para manter a proteção e resiliência.

Dividimos este guia em três partes: **Análise pré-contrato, Lista de verificação do contrato e Orientações para analisar o contrato.**

info@cyberreadinessinstitute.com

Análise pré-contrato

Antes de entrar numa discussão detalhada do contrato, é importante conhecer as prioridades, os antecedentes e a experiência do seu potencial fornecedor. Estes são alguns itens-chave a investigar sobre o fornecedor proposto ANTES de assinar o contrato. Não há uma resposta "correta" às perguntas seguintes. Estas pretendem ajudá-lo a compreender o nível de sofisticação do fornecedor.

Perguntas a fazer ao fornecedor

1. Identifique os pontos de contacto no fornecedor para serviços específicos e quem vai ser o seu gestor de relações.
2. Verifique se os colaboradores desse fornecedor fizeram as devidas verificações de segurança (como verificações de antecedentes) para lidar com informações privadas.
3. Confirme se o seu fornecedor possui cibersegurança e verifique a dimensão e o limite de cobertura em caso de incidentes cibernéticos na sua empresa. Isto ajuda a identificar possíveis lacunas em cobertura entre o seguro do fornecedor e o seguro que possa já ter ou não.
4. Pergunte-lhe sobre o respetivo nível de controlos de segurança e se estes estão alinhados com padrões ou enquadramentos (por exemplo, certificações ou credenciais como NIST 800-53, NIST Cybersecurity Framework, ISO27001, FedRamp e/ou relatórios de auditoria como um SOC2).
5. Saiba qual é o horário de funcionamento do suporte técnico (por exemplo, é um horário de serviço normal ou 24 horas por dia, 7 dias por semana?) Qual é a disponibilidade pós-laboral do fornecedor?
6. Se este aloja software ou dados, saiba onde estão alojados e quem controla esses servidores, e peça aos fornecedores para os notificar sobre quaisquer alterações. Em alguns casos, o fornecedor pode dar-lhe apoio só a si, sem alojar o seu software ou dados.
7. Determine se o fornecedor utiliza outros serviços de outras empresas ou entidades subcontratadas para lhe prestar o serviço.
8. Pergunte se o fornecedor faz parte de algum serviço ou organização que presta serviços de informação sobre ameaças.

Lista de verificação do contrato

Apresentamos a seguir algumas orientações sobre como avaliar o contrato com o seu fornecedor de cibersegurança. Na tabela seguinte, damos sugestões sobre os serviços obrigatórios que devem ser especificados no contrato, bem como alguns elementos opcionais que deve ter em conta.

Obrigatório

- ☐ Disponibilidade de assistência ao cliente: horário de apoio disponível incluído no pacote de preços básico
- ☐ Documentação e guias de utilizadores para hardware e software relevantes
- ☐ Configuração de hardware (como servidores, portáteis, Wi-Fi, smartphones)
- ☐ Instalação e atualizações de software
- ☐ Apoio técnico à rede
- ☐ Consultoria (CIO virtual)
- ☐ Cópia de segurança e recuperação (âmbito, testes, frequência)
  - **As cópias de segurança estão offline?**
  - **As cópias de segurança estão encriptadas?**
- ☐ Práticas de encriptação de dados
  - **Os dados estão encriptados em inatividade?**
  - **Os dados estão encriptados em trânsito?**
- ☐ Definição do nível de resposta por prioridade (exemplos abaixo)
  - **PRIORIDADE 1 – nível de empresa, com impacto financeiro imediato, menos de 30 minutos**
  - **PRIORIDADE 2 – problemas específicos de aplicações ou departamentos, 30 minutos a 4 horas**
  - **PRIORIDADE 3 – uma pessoa afetada, 4 a 8 horas**
- ☐ Cláusula de reencaminhamento ao fornecedor em caso de problemas não resolvidos
- ☐ Contactos principais de resposta a incidentes (fornecedor e cliente)
- ☐ Expectativas mínimas para controlos de segurança
  - **Active Directory ou configuração equivalente para controlo de acesso**
  - **Configuração de rede**
  - **Timing das atualizações (por exemplo, o fornecedor corrige vulnerabilidades críticas em 1 a 3 dias úteis)**
  - **O fornecedor notifica se houver uma violação de segurança no prazo estipulado**
  - **Objetivo de alojamento e tempo de atividade, incluindo um tempo máximo de inatividade**
  - **Visibilidade sobre onde os dados são armazenados**
  - **Processo e calendário de integração**
- ☐ Cláusula de rescisão de serviços

Opcional

- ☐ Administrador/Arquiteto do sistema e rede
- ☐ Serviços de consultoria (não especificados noutra cláusula) e partilha de boas práticas do setor
- ☐ Apoio a colaboradores em teletrabalho
- ☐ Apoio a colaboradores com dispositivos pessoais
- ☐ Apoio pós-laboral
- ☐ Poder de compra (descontos em hardware e software por compras em volume)
- ☐ Verificação de registos (frequência)
- ☐ Frequência e âmbito dos relatórios de atividade da rede
- ☐ Participação em exercícios de resposta cibernética, incluindo formação em simulação e resposta a incidentes
- ☐ Formação (tipo e frequência, como autenticação multifator, VPN, transferência de dados segura, etc.)
- ☐ Assistência no desenvolvimento de um plano de resposta a incidentes
  - **Responsabilidade e funções em caso de incidentes**
  - **Custos adicionais associados a um incidente**

info@cyberreadinessinstitute.com

Orientação para analisar o contrato

Algumas questões são negociáveis, mas deve garantir que sabe o que procura num fornecedor e identificar o tipo correto de fornecedor antes de celebrar um contrato formal. Se precisar de ajuda na escolha do tipo de fornecedor correto, releia os **guias anteriores** nesta série.

Segue abaixo um excerto de exemplo de um contrato que descreve a abordagem geral de um fornecedor à relação e o serviço prestado. Nem todos os prestadores de serviços fornecem este nível de detalhe sobre a sua abordagem, mas esta pode ser uma referência para si sobre alguns dos elementos gerais a ter em conta:

> "A nossa Equipa e o centro de apoio também trabalham em gestão de redes, sendo um ponto focal para todas as necessidades de gestão de contratos com fornecedores. **Além disso, facultamos uma equipa competente, a infraestrutura e os recursos de design e desenvolvimento Web e de software para projetos como sites baseados em bases de dados**. A [MSP] tem uma abordagem proativa e personalizada à resolução de problemas. A missão da [MSP] inclui proporcionar um ambiente profissional e amigável para o cliente em termos de **apoio e administração do sistema no local** Para realizar essa missão, temos a combinação certa de pessoas, processos e tecnologias. A nossa abordagem permite-nos prestar o melhor nível de apoio ao cliente, graças ao nosso pessoal no local e remotamente pelo Centro de apoio. **Implementamos documentação personalizada e tecnologias de qualidade, com regras empresariais específicas**, **fluxos de trabalho e catálogos de dispositivos/acessórios/tarifas, para lhe fornecer tecnologias de implementação de políticas**. Outros serviços prestados pela nossa empresa: A [MSP] dá alternativas para **resolução de problemas de servidores e áreas de trabalho de grande dimensão** e apoio, **dispositivos sem fios**, garantia de informações, **encriptação de dados**, **proteção e prevenção de firewall**, ligações de TI seguras, dados biométricos, gestão de projetos de TI, **call center**, controlo de apoio e recursos de TI, **vigilância Web**."

A página seguinte contém um excerto de disposições contratuais específicas. Tenha em atenção o nível de detalhe no timing dos serviços e a especificidade sobre a responsabilidade dos clientes:

APRESENTAÇÃO DE DESCRIÇÃO DO TRABALHO No. S1-2017-205-433

Sujeito aos termos do Contrato de Serviços Profissionais ("Contrato"), as Partes celebram a presente Descrição do Trabalho ("DT").

Rescisão

1. Período de prestação: O Período de prestação inicial será de 1 de novembro de 2018 a 30 de novembro de 2019. A menos que uma das Partes entregue um aviso por escrito de rescisão antes do final do Período de prestação inicial, o Contrato continuará, de mês a mês, até que uma Parte dê um aviso por escrito de rescisão nos termos do Contrato.

Horário padrão da assistência ao cliente

2. Serviços: Os Serviços serão realizados no local ou remotamente, a exclusivo critério da [MSP], principalmente no local do Cliente. Será dado um apoio padrão entre as 09:00 e as 18:00, fuso horário EST, de segunda a sexta, exceto em feriados celebrados pelo Cliente. O apoio de emergência pós-laboral e a monitorização de rede serão prestados 24 horas por dia, 7 dias por semana, 365 dias por ano.

Rapidez de serviço

3. 2.1 Serviços abrangidos 2.1.1. **Assistência ao cliente:** A [MSP] facultará um sistema de tickets (ConnectWise) e uma ferramenta de **Gestão de monitorização remota** (RMM) (N-able), bem como um antivírus (Sophos). O cliente irá submeter todos os seus problemas através do portal de cliente online, por e-mail ou linha telefónica. O cliente poderá receber apoio por e-mail, telefone ou remotamente, para resolver quaisquer problemas informáticos que possam atrasar a produtividade. **No caso de emergência no local, um técnico da [MSP] dará confirmação no prazo de 30 minutos e iniciará a deslocação ao local em 2 horas.** Qualquer manutenção não urgente no local será agendada entre a [MSP] e o Cliente, mas poderá ser solicitado que a [MSP] **faça o serviço no caso de 4 horas laborais, caso o Cliente determine que tal seja necessário para retomar as operações de TI.** A [MSP] responderá no local em instalações do Cliente na zona de [city] e as deslocações NÃO serão consideradas como custo adicional. A [MSP] irá gerir o e-mail do cliente, através da gestão de utilizadores finais ao adicionar ou remover contas de e-mail, perfis de utilizadores e configuração de computadores. O Cliente tem de dar um aviso prévio de 5 dias úteis antes da configuração de novos utilizadores ou remoção dos mesmos. O Cliente irá preencher o modelo no portal do Cliente fornecido pela [MSP] para novos utilizadores e rescisão de utilizadores."

Este guia foi feito para o ajudar a rever e compreender potenciais contratos antes de celebrar um contrato formal com um fornecedor. No próximo e último guia desta série, vamos falar de como gerir a relação contínua depois de ter assinado o contrato. Lembre-se de que a finalidade do contrato é definir expectativas para criar uma relação de confiança entre si e o seu prestador de serviços.

A lista completa de guias desta série:

Devo obter suporte externo para gerir o meu risco de segurança cibernética?

Introdução aos tipos de suporte externo de TI e segurança cibernética

Como selecionar o nível certo de suporte externo

Revisão e compreensão do contrato

(ESTE GUIA)

As suas responsabilidades contínuas de segurança cibernética

Autores que contribuíram

- 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

Sobre o CRI

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de iniciação ou crie uma cultura de preparação cibernética na sua empresa com o Programa de preparação cibernética online. Os nossos recursos de teletrabalho e guias de local de trabalho híbrido oferecem sugestões oportunas para lidar com a evolução dos desafios cibernéticos da atualidade. Para saber mais, visite **www.BeCyberReady.com**.