

# GUIA DO NÍVEL CISO: PROTEGER LIGAÇÕES A TERCEIROS

## IDENTIFICAÇÃO DE RISCO ATRAVÉS DE TERCEIROS

- Crie e mantenha uma lista atualizada de todas as relações com fornecedores e os ativos e dados expostos em cada uma.
- Reveja os dados a que cada fornecedor ou terceiro tem acesso. Certifique-se de que este nível de acesso adere ao princípio de “privilégios mínimos”.
- Classifique o seu fornecedor e as relações com terceiros (baixo, médio, alto) com base no impacto que uma violação dos seus sistemas teria na sua organização.
- Começando pelos fornecedores de maior risco, avalie as capacidades de cibersegurança de cada fornecedor. O cumprimento das normas relevantes é um bom ponto de partida. Desenvolver um plano para avaliação de segurança regular. Pode querer ocasionalmente realizar avaliações no local de fornecedores com o maior risco e/ou maior acesso aos dados do cliente.

## GESTÃO DE SEGURANÇA DE TERCEIROS

- Realizar diligência devida rigorosa. Estabeleça expectativas de cibersegurança nos pedidos da sua organização para propostas, contratos, continuidade do negócio, resposta a incidentes e acordos de nível de serviço com fornecedores. Acordar responsabilidades e obrigações em caso de acidente cibernético.
  - Inquirir sobre as práticas de cibersegurança de outros terceiros, tais como organizações financeiras com as quais realiza transações ou partilha dados. Quaisquer requisitos de cibersegurança aos quais a sua organização devem aderir deve também ser seguidos pelos seus fornecedores e quaisquer outras organizações com as quais partilhe dados ou exponha ativos.
- Utilize medidas estabelecidas e acordadas para monitorizar a conformidade dos seus fornecedores com os padrões de cibersegurança.
- Consulte os seus fornecedores que lidam com dados sensíveis para ver se oferecem autenticação de dois fatores, encriptação ou outras medidas de segurança para quaisquer contas que tenha com os mesmos.
- Certifique-se de que todo o software e hardware de terceiros que instalar têm um aperto de segurança para que os processos de arranque sejam protegidos através de códigos de autenticação e não serão executados se os códigos não forem reconhecidos.
- Se encontrar produtos de fornecedores que sejam falsificados ou não correspondam às especificações, trabalhe no sentido de negociar uma resolução ou outra estratégia de saída.
- Avalie anualmente contratos de fornecedores e certifique-se de que estes continuam a cumprir os requisitos de segurança de dados regulamentares e da direção. Após a rescisão do contrato, inclua estipulações sobre a obtenção dos seus ativos ou dados e verifique que os ativos ou dados são totalmente apagados no lado do fornecedor e desativam o acesso aos seus sistemas ou servidores.

## PARTILHAR INFORMAÇÕES

- Certifique-se de que tem canais de comunicação claros e pontos de contacto para comunicar sobre questões de segurança com os fornecedores e contrapartes da sua organização.
- Envolve-se na partilha atempada de informações de cibersegurança fiáveis e acionáveis com partes interessadas internas e externas (incluindo entidades e autoridades públicas dentro e fora do setor financeiro).
- Monitorize as atualizações relevantes sobre o que outras organizações estão a experienciar com os seus terceiros em termos de ameaças, vulnerabilidades, incidentes e respostas para melhorar as defesas da sua organização, aumentar a perceção das situações e alargar a aprendizagem. Fazer parte das organizações que partilham informações, por exemplo, o FS-ISAC, facilitará estar atualizado.

## Como escolher fornecedores com cibersegurança em mente

Coloque as seguintes perguntas de potenciais fornecedores para avaliar a sua preparação e consciencialização cibernética e, consequentemente, o impacto que teriam no perfil de risco da sua organização:

1. Que experiência têm? Saiba mais sobre a história do fornecedor que serve os clientes. Já serviram clientes semelhantes à sua organização?
2. Documentaram a sua conformidade com os padrões de cibersegurança conhecidos como o Quadro NIST ou ISO 27001, ou podem fornecer um relatório SOC2?
3. Quais dos seus dados e/ou ativos terão de aceder para prestar os seus serviços? Estão a solicitar algum acesso aparentemente desnecessário?
4. Como planeiam proteger os ativos e dados da sua organização que estão na sua posse?
5. Como gerem o seu próprio risco cibernético de terceiros? Podem fornecer informações sobre a sua cadeia de abastecimento?
6. Qual é o seu plano para recuperação de desastres e continuidade de negócios no caso de um incidente ter impacto nos ativos e/ou dados da sua organização?
7. Como irão manter a sua organização atualizada? Qual é o seu plano para comunicar tendências, ameaças e alterações na sua organização?