Mitigação do Risco Cibernético de Terceiras Partes para uma Segurança Empresarial Reforçada

Abordar de forma eficaz as potenciais ameaças apresentadas por fornecedores de terceiras partes permite à sua organização manter o foco nas principais atividades do negócio.

devoteam
Cyber Trust

No mundo digitalmente interligado de hoje, as empresas dependem amplamente de fornecedores de serviços para realizar funções e serviços críticos. Estes fornecedores podem ter acesso a dados sensíveis, redes e sistemas, tornando-se potenciais pontos de entrada para ataques cibernéticos. Infelizmente, muitas empresas não possuem os recursos ou conhecimentos necessários para gerir eficazmente o risco cibernético de terceiras partes por conta própria.

É aqui que entra a gestão de risco cibernético de terceiras partes. Trata-se de um processo de identificação, avaliação e mitigação dos riscos cibernéticos associados a serviços fornecidos por terceiras partes. A gestão de risco cibernético de terceiras partes ajuda as empresas a garantir que os seus fornecedores de serviços implementam controlos de segurança adequados e cumprem normas e regulamentos da indústria.

À medida que os ataques cibernéticos são cada vez mais sofisticados e frequentes, a necessidade de gestão de risco cibernético de terceiras partes tornou-se cada vez mais crítica nos últimos anos. Estes ataques podem resultar em violações de dados, perdas financeiras, danos à reputação e multas regulatórias. A implementação de um programa robusto de gestão de risco cibernético de terceiras partes pode ajudar as empresas a protegerem as suas informações sensíveis, reduzir o risco de ataques cibernéticos e manter a confiança dos seus clientes e partes interessadas.

Em geral, a gestão de risco cibernético de terceiras partes é essencial para qualquer empresa que dependa dos fornecedores para garantir a segurança dos seus sistemas e dados. **Ao gerir o risco cibernético de terceiras partes, as empresas podem identificar e abordar proativamente potenciais vulnerabilidades antes que se tornem incidentes de segurança significativos.**

Experiência da Devoteam Cyber Trust

Na Devoteam Cyber Trust, temos mais de 15 anos de experiência em fornecer serviços de segurança ofensiva de ponta e engenharia de cibersegurança para organizações de todos os tamanhos, numa ampla gama de setores. Os nossos consultores especializados são altamente qualificados e certificados em standards do setor, como PCI QSA, CISSP, CCSP e ISO 27001, e têm um amplo conhecimento das últimas metodologias e ferramentas utilizadas por potenciais atacantes.

Com as nossas estratégias de gestão de risco de terceiras partes, aliadas à nossa capacidade de adaptação às necessidades específicas de cada cliente e à nossa plataforma de gestão, proporcionam uma visibilidade contínua relativamente à sua postura de segurança, possibilitando assim a identificação e mitigação proativa de potenciais vulnerabilidades e riscos.

Ao trabalhar connosco, pode ter a confiança que estará associado a um parceiro experiente no campo da Gestão de Risco Cibernético de Terceiras Partes.

(*) De acordo com um relatório recente da IBM Security e do Ponemon Institute, o custo médio de uma violação de dados em 2021 foi de US$ 4,24 milhões, ou aproximadamente 3,53 milhões de euros.

TPCRM

Normas e Regulamentações

Além dos benefícios operacionais na identificação e mitigação de potenciais riscos, a Gestão de Risco Cibernético de Terceiras Partes, também conhecida na sigla inglesa como TPCRM, está a tornar-se cada vez mais importante para as organizações do ponto de vista regulamentar e de conformidade.

Ao envolverem-se numa TPCRM, as organizações podem demonstrar o seu compromisso em cumprir os requisitos regulamentares e de conformidade, bem como alinhar-se com as melhores práticas para a gestão da segurança da informação.

- **ISO 27001:** O Anexo A desta norma contém um conjunto de controlos relacionados com a gestão de risco de segurança da informação, incluindo requisitos para a gestão de riscos de fontes externas, como fornecedores.
- **NIS2:** A Diretiva NIS2 obriga as entidades a garantir a segurança das suas redes e sistemas de informação, incluindo os dos seus fornecedores de terceiras partes.
- **NIST CSF:** Embora o NIST CSF não obrigue a uma TPCRM, reconhece a importância crítica de gerir riscos de cibersegurança relacionados com parceiros de terceiras partes. Implementar uma TPCRM pode ser um componente valioso da estratégia global de cibersegurança de uma organização, alinhando-se com os princípios e orientações delineados no NIST CSF.
- **PCI-DSS:** O PCI DSS v4.0 inclui requisitos específicos para uma TPCRM, a fim de garantir a segurança dos dados do titular do cartão em toda a cadeia de fornecimento da indústria de cartões de pagamento. As organizações que aceitam cartões de pagamento devem implementar um programa robusto de TPCRM para gerir os riscos de cibersegurança associados a prestadores de serviços de terceiras partes e cumprir os requisitos do PCI DSS.
- **Regulamento Geral de Proteção de Dados (RGPD):** O RGPD é um regulamento da União Europeia que estabelece regras rigorosas para a proteção de dados pessoais. Exige que as organizações garantam medidas de segurança adequadas para o processamento de dados, incluindo quando trabalham com terceiras partes.

"Mesmo quando a culpa é de terceiros, a responsabilidade continua a ser sua."

Trata-se de compatibilidade.

À medida que os ataques cibernéticos continuam a ser uma ameaça constante, a questão não é se irá ocorrer um ataque, mas sim quando.

Para gerir efetivamente esse risco, as organizações precisam de adotar uma abordagem proativa em relação à cibersegurança, incluindo a gestão do risco cibernético herdado das terceiras partes.

A nossa abordagem para mitigar os riscos de cibersegurança apresentados pelas suas terceiras partes

Para maximizar os benefícios do seu investimento na gestão de risco cibernético de terceiras partes, é importante manter uma supervisão constante das ações necessárias e garantir que o plano acordado e os prazos sejam comunicados a todas as partes envolvidas.

Além disso, adotar um sistema que seja flexível e que possa crescer com a sua organização é fundamental, uma vez que a melhoria contínua é um aspeto-chave de qualquer processo eficaz de gestão de riscos. O sistema de suporte deve ser ágil e adaptável para satisfazer as necessidades em constante evolução da sua organização.

Apoiar fornecedores de terceiras partes na implementação de controlos de cibersegurança eficazes e práticas de gestão de risco é essencial, uma vez que essas entidades podem ter acesso a dados sensíveis, redes e sistemas. Se os seus controlos de cibersegurança forem fracos ou inadequados, podem tornar-se pontos de entrada para ciberataques, permitindo o acesso não autorizado aos dados e sistemas da organização

Ao fornecer apoio e orientação às terceiras partes, as organizações podem ajudar a garantir que elas estão a implementar controlos de segurança adequados e a cumprir os padrões da indústria e as regulamentações.

Para gerir eficazmente o risco cibernético de terceiras partes, é importante identificar o valor de negócio e o potencial impacto de cada terceira parte, bem como atribuir um nível de criticidade correspondente, dado que ao atribuir o mesmo nível de criticidade a todas as terceiras partes, pode dificultar a capacidade de avaliá-las.

Mantenha um inventário organizado de todas as avaliações, evidências de suporte e relatórios.

Adote um sistema que possa acompanhar todas as informações recolhidas e informar os responsáveis de quaisquer ações necessárias.

O que abordamos na nossa revisão de Terceiras Partes

Identificar e avaliar 3as partes

Identificar e avaliar todas as 3as partes no âmbito, tendo em consideração a atividade da organização e de acordo com a sua relevância.

Executar o programa de avaliação e recolha de evidências

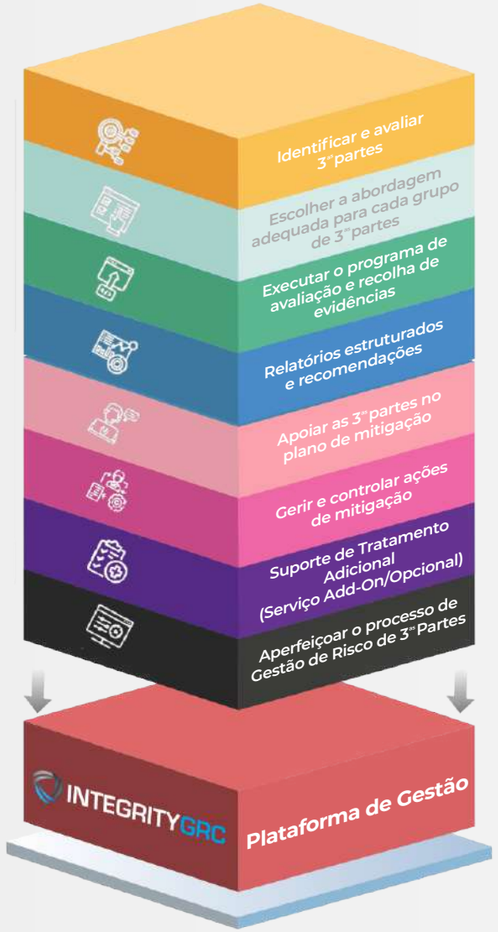
Um programa de avaliação pré-definido será realizado por meio de entrevistas e recolha de evidências, com a apresentação executiva e técnica dos resultados.

Apoiar as 3as partes no plano de mitigação

Todas as partes relevantes que participam no processo de mitigação e recebem apoio da Devoteam Cyber Trust serão capazes de gerir e manter o plano de mitigação na plataforma IntegrityGRC.

Suporte de Tratamento Adicional (Serviço Add-On/Opcional)

A Devoteam Cyber Trust irá participar em nome do cliente para interagir com terceiras partes internas/externas a fim de uma gestão eficaz do processo de mitigação.



Escolher a abordagem adequada para cada grupo de 3as partes

Definir o programa/plano de avaliação com os cenários para cada grupo de 3as partes.

Relatórios estruturados e recomendações

Um especialista em cibersegurança irá contextualizar as questões identificadas e definir recomendações para a sua mitigação. Todas as descobertas serão relatadas na plataforma IntegrityGRC.

Gerir e controlar ações de mitigação

As organizações serão capazes de gerir e controlar as ações de mitigação na plataforma IntegrityGRC, bem como todo o ciclo de vida das descobertas.

Aperfeiçoar o processo de Gestão de Risco de 3as Partes

Avaliar as lições aprendidas e definir otimizações para um ajuste contínuo do processo de Gestão de Risco de Terceiras Partes da Devoteam Cyber Trust.

Planos de Serviço

Cada organização tem um conjunto de terceiras partes que fornecem serviços distintos à organização, mas nem todos eles são equivalentes em termos de importância ou potencial impacto para a organização.

O serviço oferece a possibilidade de selecionar o número e os tipos de terceiras partes, de acordo com os seguintes serviços:

Terceiras Partes	Avaliação de Conformidade Cibernética	Avaliação Técnica
Tipo 1	• **Estrutura de Análise:** Até 50 perguntas da base de dados de perguntas do modelo de categorias de segurança da informação.	• N/A
Tipo 2	• **Estrutura de Análise:** Até 100 perguntas da base de dados de perguntas do modelo de categorias de segurança da informação.	• **ICSSC (Integrity Cybersecurity Scorecard):** O ICSSC da Devoteam Cyber Trust contém um conjunto de controlos de cibersegurança a serem avaliados em relação ao ambiente de cibersegurança da organização. Uma vez executado, fornece uma visão clara e objetiva da postura de cibersegurança da organização.
Tipo 3	• **Estrutura de Análise:** Perguntas personalizadas a partir da base de dados de perguntas do modelo de categorias de segurança da informação e/ou perguntas específicas do cliente.	• **ICSSC (Integrity Cybersecurity Scorecard);** • **Verificações técnicas completas:** Revisão da arquitetura de segurança, verificações técnicas detalhadas e aprofundadas para cada 3a parte/tecnologia; • **Integrações externas:** Pode incluir outros serviços fornecidos pela Devoteam Cyber Trust, como teste de penetração (pen-test).

Relatórios Entregáveis

Na Devoteam Cyber Trust, disponibilizamos relatórios formais e dinâmicos para os nossos serviços de TPCRM (Gestão de Risco Cibernético de Terceiras Partes).

Relatório Formal por Terceira Parte

1. **Resumo Executivo:** Uma visão geral de alto nível das principais descobertas, incluindo vulnerabilidades identificadas, riscos e recomendações.
2. **Descobertas:** Uma análise detalhada das descobertas identificadas, incluindo gravidade, impacto e probabilidade de exploração, bem como potenciais vetores de ataque e cenários.
3. **Recomendações:** Recomendações específicas para remediação e mitigação das descobertas identificadas, incluindo soluções técnicas, melhorias de processo e iniciativas de formação ou educação.
4. **Conclusão:** Um resumo das principais descobertas e recomendações, bem como quaisquer informações ou observações adicionais resultantes do envolvimento.
5. **Apêndices:** Informações técnicas adicionais, tabelas, gráficos e outros dados de suporte para complementar as descobertas e recomendações no relatório principal.

// A estrutura pode variar dependendo do serviço específico.

Dinâmico

A nossa poderosa plataforma IntegrityGRC fornece todas as descobertas e todas as ferramentas para gerir o processo de remediação. Pode gerir globalmente o risco das suas Terceiras Partes ou por grupos ou indivíduos.

Conheça os Benefícios

- **Melhoria na postura de segurança:** A TPCRM ajuda as organizações a identificar e avaliar potenciais riscos de cibersegurança associados a fornecedores de terceiras partes, permitindo a mitigação proativa de riscos e o fortalecimento da postura de segurança global.

- **Redução do risco de ataques cibernéticos:** Uma TPCRM eficaz pode ajudar a reduzir o risco de ataques cibernéticos através de canais de terceiras partes, prevenindo violações de dados, perdas financeiras e danos à reputação.

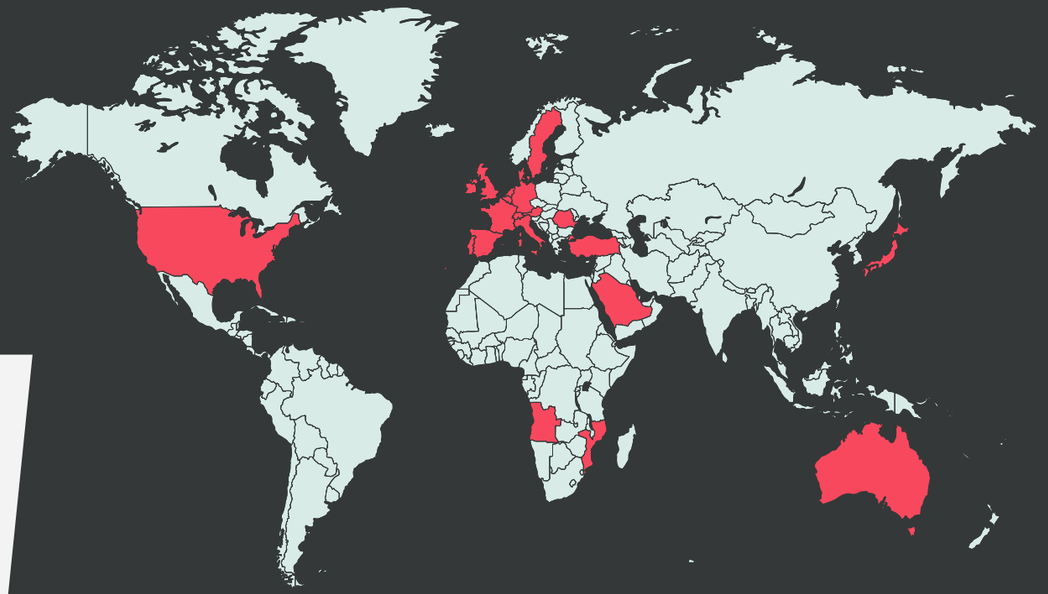
- **Conformidade com regulamentações:** Muitas regulamentações e padrões da indústria, como a Diretiva NIS2 e o PCI DSS, exigem a implementação de TPCRM. A implementação da TPCRM ajuda as organizações a cumprir essas regulamentações e a evitar possíveis multas e penalidades.

- **Aumento da confiança com partes interessadas:** Ao gerir eficazmente os riscos de cibersegurança de terceiras partes, as organizações podem manter a confiança dos seus clientes, parceiros e partes interessadas, protegendo as suas informações e dados sensíveis.

- **Economia de custos:** A implementação da TPCRM pode ajudar as organizações a evitar incidentes dispendiosos de cibersegurança causados por vulnerabilidades de terceiras partes e a reduzir os custos associados à gestão desses incidentes.

Certificações & Clientes

Apoiada numa carteira diversificada de clientes globais e numa ampla gama de certificações, incluindo CREST, ISO 27001, ISO 27701, ISO 9001 e PCI QSA, a Devoteam Cyber Trust é a principal opção para organizações que procuram o mais alto nível de especialização em serviços de risco cibernético de terceiras partes.



Mais de 20 países em todo o mundo

Com sede em Lisboa, prestamos serviços a um grande **número de empresas de grande e média dimensão**, tanto a nível nacional como internacional.

Casos de Estudo

Gestão de Risco de Parceiros Estratégicos

Tipo de Cliente: Farmacêutica/Biotecnologia com mais de 15.000 funcionários e presença global

Desafio: O Cliente possui um conjunto de parceiros estratégicos que fornecem soluções tecnológicas, principalmente no modelo CaaS (Cloud as a Service), e o cliente não tinha a estrutura nem o conhecimento aprofundado para realizar regularmente a avaliação da postura de cibersegurança dos seus parceiros e os potenciais riscos que possam surgir disso.

Gestão de Risco de Conformidade

Tipo de Cliente: Empresa Agroindustrial Global com mais de 11.000 funcionários em 37 países

Desafio: Numa empresa agroindustrial de destaque, um conjunto extenso de terceiras partes exigia avaliações de conformidade como parte de um processo mais amplo de Gestão de Risco Cibernético de Terceiras Partes (TPCRM) com várias camadas. O desafio consistia em conduzir eficientemente estas avaliações iniciais para identificar terceiras partes de alto risco para avaliações mais detalhadas, ao mesmo tempo que se minimizavam os recursos e o tempo despendido com terceiras partes de baixo risco.

Avaliação de Fornecedores

Tipo de Cliente: Entidade Financeira com mais de 35.000 funcionários e presença global

Desafio: Numa organização financeira de grande dimensão, existe a necessidade de um processo sólido de avaliação de fornecedores como parte da sua estratégia de Gestão de Risco Cibernético de Terceiras Partes (TPCRM). O desafio reside em avaliar com precisão o perfil de risco de cada fornecedor, garantindo que cumpram estritos padrões de segurança e conformidade, ao mesmo tempo que mantêm a eficiência no processo de avaliação.

O que os nossos clientes dizem sobre nós

"

O projeto é um sucesso, a equipa tem muito conhecimento técnico, superou as expectativas.

SAÚDE

"

Este é um serviço win-win e o nível de análise é incrível.

ENERGIA

"

É muito fácil trabalhar com a Devoteam Cyber Trust.

BANCO

Clique aqui para saber mais sobre estes e outros casos de estudo, as soluções aplicadas e o impacto.

Porquê trabalhar com a Devoteam Cyber Trust

- Profundo conhecimento e experiência em Engenharia de Cibersegurança, com mais de 15 anos de experiência líder na indústria.
- Uma equipa de profissionais de segurança altamente certificados e experientes, com certificações como CISSP, CCSP, Lead Auditor ISO 27001, PCIP e PCI QSA.
- Compromisso com qualidade e excelência, com foco na entrega dos mais altos níveis de serviço e satisfação do cliente.
- Acesso à tecnologia e ferramentas avançadas, que inclui uma plataforma IntegrityGRC proprietária.
- Conformidade com padrões e regulamentos do setor, incluindo PCI-DSS, ISO 27001, NIS2, RGPD e outras diretrizes e normas relevantes.
- Foco em parcerias de longo prazo e suporte contínuo, com melhoria contínua dos serviços oferecidos.
- Presença global e reputação, com clientes em mais de 20 países e um histórico comprovado de fornecer serviços eficazes e de alta qualidade de testes de segurança ofensiva.

Como Começar

01

Agende uma conversa inicial com os nossos consultores especializados para discutir as suas necessidades, objetivos e preocupações.

02

Analise e aprove a nossa proposta personalizada delineando o âmbito dos nossos serviços, prazos e custos.

03

Finalize os detalhes da proposta, incluindo metodologias e âmbito de testes.

04

Obtenha informações em tempo real sobre os seus riscos e vulnerabilidades de segurança através da nossa plataforma de gestão de vulnerabilidades.

05

Receba atualizações regulares sobre o nosso progresso, incluindo relatórios detalhados e recomendações de remediação.

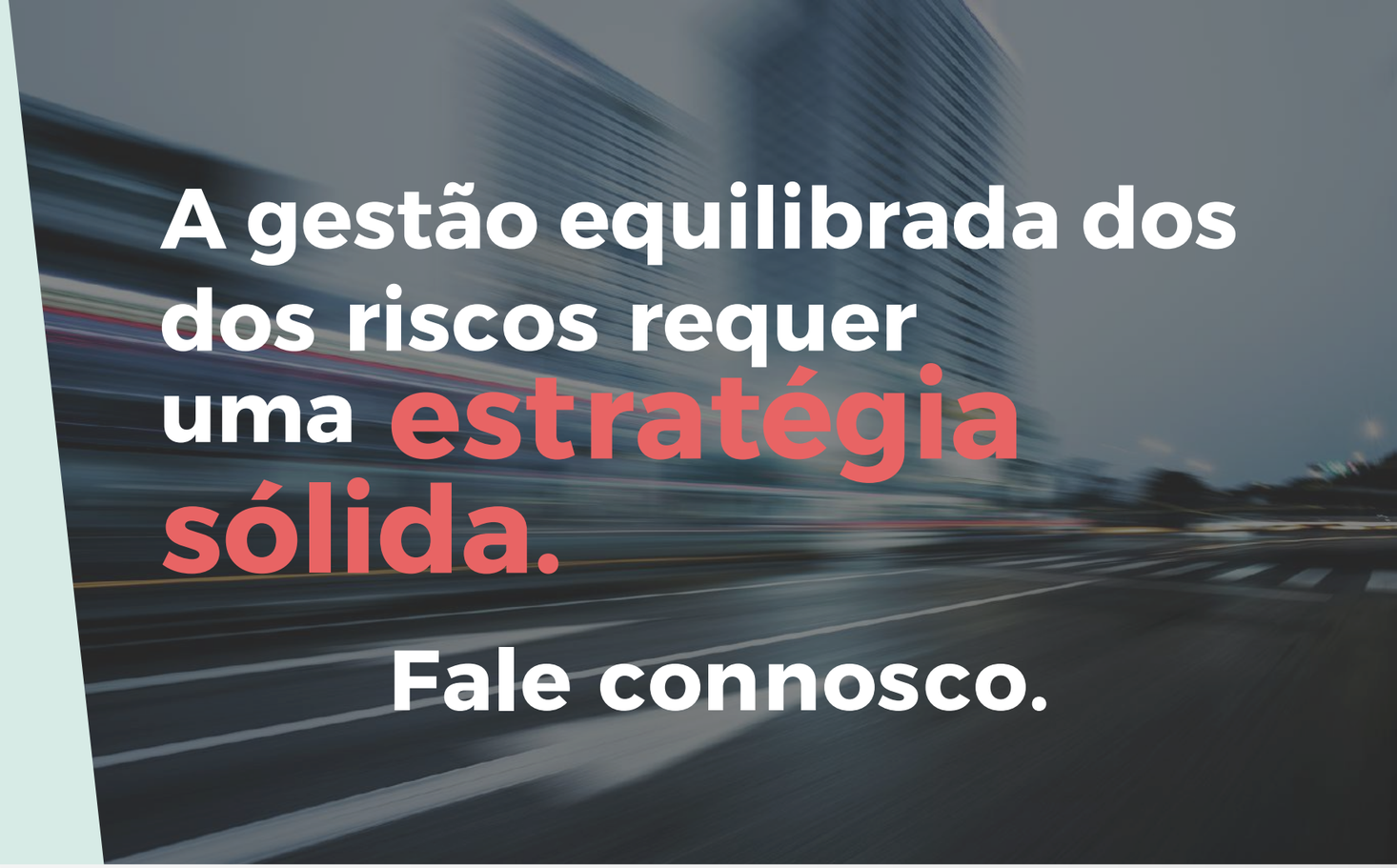
06

Receba suporte e orientação contínuos da nossa equipa, conforme necessário.

Devoteam Cyber Trust é o parceiro certo para apoiar a sua organização neste cenário de ameaças intenso e em constante evolução, com Serviços de Segurança Ofensiva de classe mundial.

É por isso que dezenas de clientes de média e grande dimensão em mais de 20 países em todo o mundo confiam nos nossos serviços.

Estamos disponíveis para partilhar a nossa **experiência** e ajudá-lo a melhorar as suas **práticas de cibersegurança.**



A gestão equilibrada dos dos riscos requer uma estratégia sólida.

Fale connosco.

Contacte-nos

info@integrity.pt

Presentes em mais de 12 países da EMEA

www.integrity.pt

devoteam Cyber Trust

Sobre devoteam Cyber Trust

www.integrity.pt

www.devoteam.com/expertise/cyber-trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados na região EMEA, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias.

Desde 2009, anteriormente com a denominação INTEGRITY, a nossa equipa sediada em Portugal é especializada em fornecer Serviços Geridos de Segurança de ponta, que combina a sua expertise e tecnologia proprietária para reduzir de forma consistente e eficaz o risco cibernético dos nossos clientes. A ampla gama de serviços abrange Testes Persistentes de Intrusão, ISO 27001, PCI-DSS, Consultoria e Soluções de GRC e Gestão de Riscos de Terceiras Partes. Certificados em ISO 27001 (Segurança da Informação), ISO 27701 (Gestão de Informação Privada) e ISO 9001 (Qualidade), PCI-QSA e membros da CREST e CIS - Centro de Segurança na Internet, prestamos serviços a um número considerável de clientes, operando em mais de 20 países.

Sobre devoteam

www.devoteam.com

A Devoteam é uma consultora líder focada em estratégia digital, plataformas tecnológicas e cibersegurança.
Ao combinar criatividade, tecnologia e insights de dados, capacitamos os nossos clientes a transformar os seus negócios e desbloquear o futuro.
Com 25 anos de experiência e 10.000 funcionários em toda a Europa, Oriente Médio e África, a Devoteam promove tecnologia responsável para as pessoas e trabalha para criar mudanças positivas.

Creative tech for Better Change