Guardians of digital trust
Cybersecurity Awareness Month

A crescente divisão entre organizações resilientes em cibersegurança e não resilientes

Como poderá a BDO ajudar a fechar esta lacuna?

BDO

A crescente divisão entre organizações resilientes em cibersegurança e não resilientes
Como poderá a BDO ajudar a fechar a lacuna?

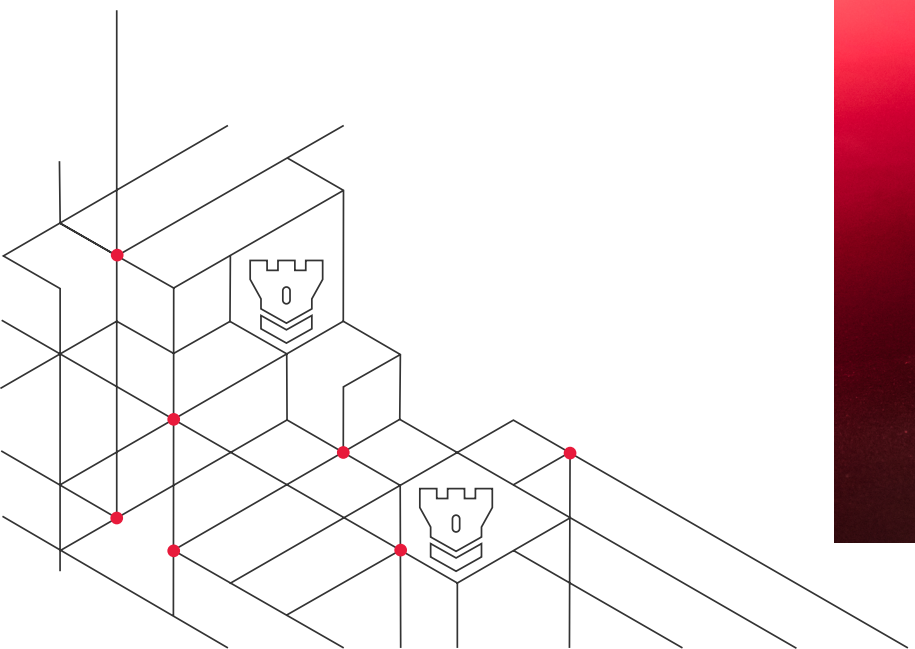
Ao longo de 2024, eventos cibernéticos, como ataques de ransomware, têm vindo a perturbar organizações em diversos sectores, incluindo a WS Audiology, na Dinamarca, a Transport for London, os casinos MGM e Caesars nos EUA, o Aeroporto SeaTac em Seattle, entre outros.

Face a esta ameaça crescente, a resiliência cibernética — a capacidade de manter as operações apesar dos ciberataques — tornou-se essencial.

Com as ameaças cibernéticas a tornarem-se cada vez mais complexas e frequentes, a lacuna entre organizações resilientes em cibersegurança e aquelas que não o são está a aumentar.

Incidentes recentes destacam os efeitos significativos dos ciberataques na reputação, finanças, operações e na confiança dos stakeholders.

O Fórum Económico Mundial classifica os ciberataques como um dos principais riscos globais, e a pandemia da COVID-19 intensificou a exposição organizacional a estes riscos.



Compreender a resiliência cibernética

A resiliência cibernética vai além da cibersegurança tradicional, que se foca principalmente na prevenção de ataques. Trata-se de uma abordagem holística, que inclui a capacidade de se preparar, responder e recuperar de incidentes cibernéticos. Uma organização resiliente em cibersegurança não só se defende contra ataques, como também garante a continuidade e uma recuperação rápida em caso de violação.

A resiliência cibernética começa muito antes de um possível incidente e exige uma gestão de riscos informada, que permita a tomada de decisões com base numa compreensão aprofundada dos riscos. Esta gestão de riscos informada envolve a recolha e análise de toda a informação relevante, a aprendizagem com os incidentes e a tomada de decisões fundamentadas para minimizar potenciais impactos negativos.

Os elementos essenciais da gestão de riscos informada são:

01

Identificação de Riscos - Reconhecer os riscos potenciais que podem afectar a organização.

02

Avaliação de Riscos - Avaliar a probabilidade e o impacto desses riscos.

03

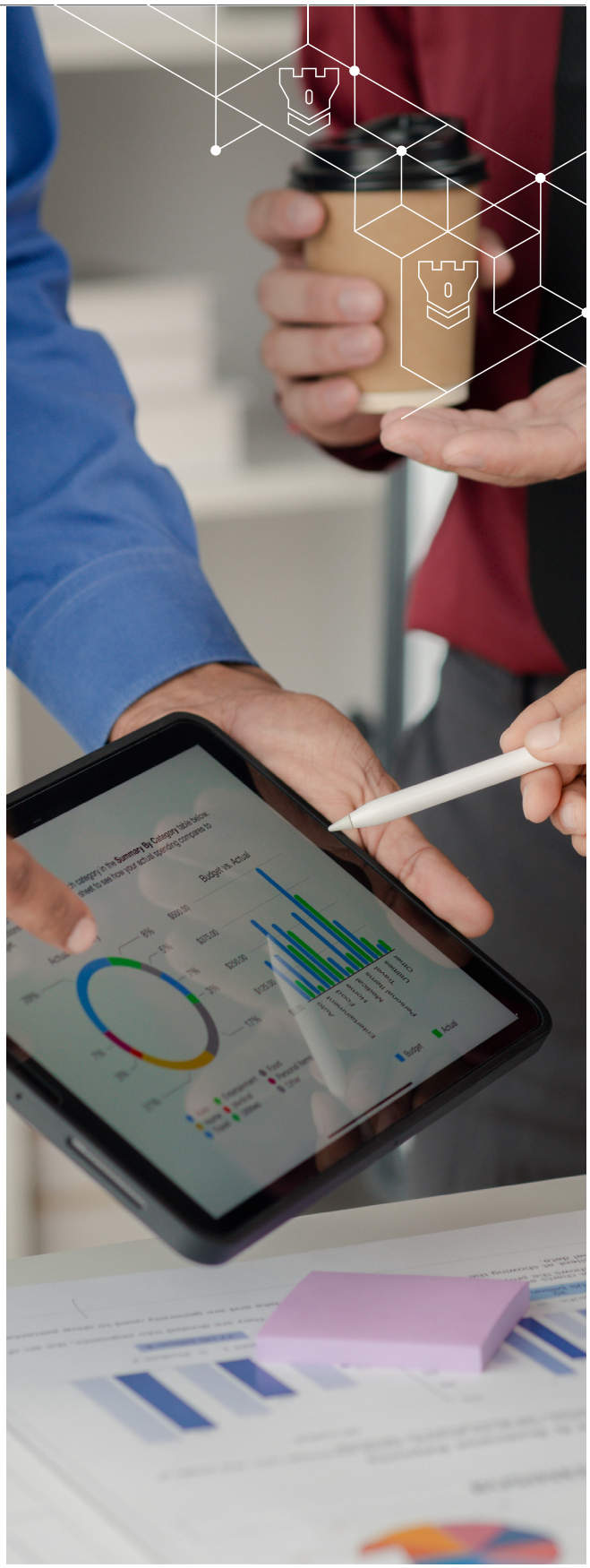
Priorização de Riscos - Determinar quais os riscos que requerem atenção imediata com base no seu impacto potencial.

04

Mitigação de Riscos - Implementar uma estratégia para reduzir ou gerir os riscos identificados.

05

Monitorização Contínua - Rever e actualizar regularmente a estratégia de gestão de riscos, adaptando-a a novas informações ou circunstâncias.



Com esta abordagem, um programa de segurança maduro opera continuamente em toda a organização.

Incluíndo:

01

Prevenção

Implementar medidas de cibersegurança robustas para prevenir ataques.

02

Deteção

Identificar e avaliar rapidamente as ameaças cibernéticas.

03

Resposta

Gerir e mitigar eficazmente o impacto dos incidentes cibernéticos.

04

Recuperação

Restaurar as operações normais rapidamente e aprender com os incidentes para fortalecer a resiliência futura.

O que é esta crescente divisão entre organizações que são resilientes em cibersegurança e aquelas que não o são?

Uma divisão significativa está a crescer entre organizações resilientes em cibersegurança e aquelas que ainda não implementaram medidas adequadas para gerir riscos de cibersegurança, conforme o mais recente relatório do Fórum Económico Mundial sobre a Perspetiva Global de Cibersegurança.

Este relatório afirma que está a emergir uma desigualdade cibernética: 90% dos executivos inquiridos na Reunião Anual de Cibersegurança do Fórum Económico Mundial no final de 2023 afirmaram ser urgente tomar medidas para abordar esta divisão.

Algumas organizações estão mais preparadas e são mais proativas na gestão dos riscos cibernéticos e na construção de resiliência cibernética.

Segundo o relatório, apenas 17% das organizações são consideradas líderes resilientes em cibersegurança, enquanto 74% ainda são novatas neste campo.

As organizações líderes têm uma estratégia cibernética clara, uma cultura cibernética forte e a capacidade de atrair talento, além de uma infraestrutura tecnológica robusta e um programa de governança eficaz. As organizações novatas, por outro lado, carecem de uma ou mais destas dimensões e estão mais vulneráveis a perturbações e perdas resultantes de violações cibernéticas.

O aumento e adoção de novas tecnologias irá amplificar os desafios já existentes, assim como a crescente lacuna de competências cibernéticas e a escassez de talento.

A Inteligência Artificial Generativa poderá aumentar a sofisticação dos ciberataques nos próximos anos, mas também será uma ferramenta valiosa para ajudar as organizações a defenderem-se.

[1] The cybersecurity trends leaders will need to navigate in 2024 | World Economic Forum (weforum.org)

A importância da resiliência cibernética

Num mundo onde os avanços tecnológicos são rápidos e as ameaças cibernéticas omnipresentes e cada vez mais sofisticadas, a importância da resiliência cibernética não pode ser subestimada. As consequências dos incidentes cibernéticos podem ser graves, desde perdas financeiras e interrupções operacionais a danos reputacionais e penalizações regulamentares.

As principais razões para investir em resiliência cibernética são:

01

Proteção Financeira

Os ciberataques podem resultar em perdas financeiras significativas. As organizações resilientes em cibersegurança estão melhor posicionadas para mitigar esses custos através de uma recuperação rápida e da continuidade das operações.

02

Continuidade Operacional

Manter as operações empresariais durante e após um ciberataque é crucial. A resiliência cibernética assegura que as funções críticas continuem a operar, minimizando o tempo de inatividade e a disrupção.

03

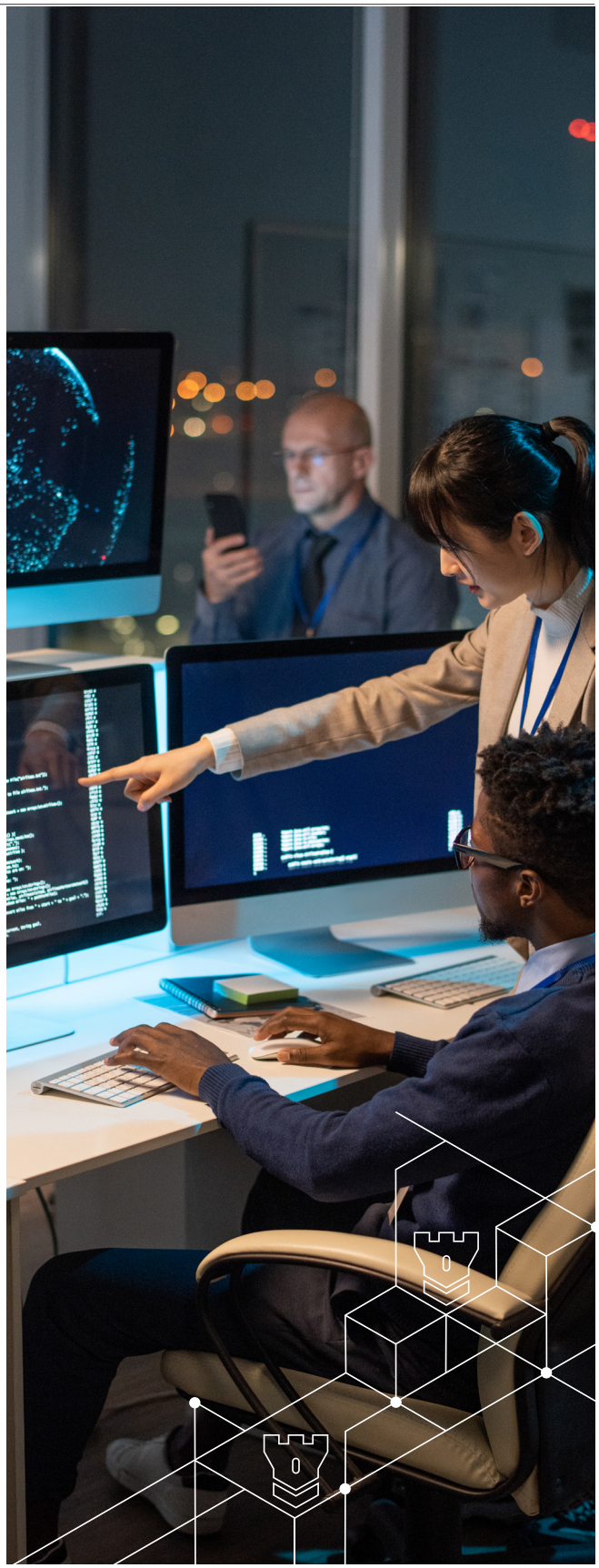
Integridade Reputacional

A confiança é um ativo valioso. As organizações que demonstram resiliência em cibersegurança têm maior probabilidade de manter a confiança e a lealdade dos clientes.

04

Conformidade Regulatória

Muitas indústrias estão sujeitas a regulamentações rigorosas em matéria de proteção de dados e cibersegurança. As organizações resilientes em cibersegurança estão melhor preparadas para cumprir estas regulamentações e evitar penalizações.



Perspetivas globais sobre resiliência cibernética

Instituições globais, como governos e o Fórum Económico Mundial (WEF), reconhecem a necessidade crítica de resiliência cibernética e oferecem orientações para ajudar as organizações a fortalecer as suas defesas.

01

Iniciativas Governamentais

- NIST Cybersecurity Framework: O Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) fornece uma estrutura abrangente para melhorar as práticas de cibersegurança, amplamente adotada em diversos setores.
- EU Directive on Security of Network and Information Systems (NIS2): Organizações em setores críticos como energia, transportes, banca e saúde serão obrigadas a implementar medidas adequadas e proporcionais para gerir riscos de segurança.
- EU Cyber Reslience Act: A Lei de Resiliência Cibernética da União Europeia visa reforçar a segurança de produtos e serviços digitais, promovendo um elevado nível de resiliência cibernética entre os estados membros.
- ASEAN: A ASEAN ainda não possui uma lei ou diretiva única e unificada de cibersegurança. No entanto, desenvolveu uma estratégia abrangente de cooperação em cibersegurança para 2021-2025, com foco em promover a prontidão cibernética, harmonizar políticas cibernéticas regionais, aumentar a confiança no ciberespaço e desenvolver a capacidade regional.
- The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) integrou a cibersegurança na sua Agenda Digital.

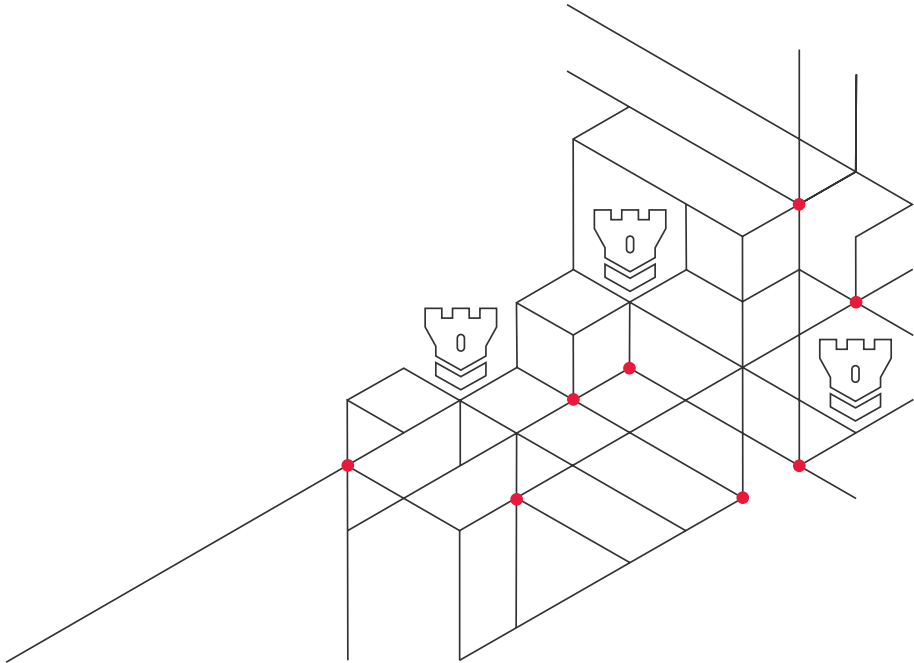
02

World Economic Forum (WEF)

- O Fórum Económico Mundial (WEF) enfatiza a importância das parcerias público-privadas para reforçar a resiliência cibernética. Os seus relatórios sublinham a necessidade de uma abordagem colaborativa para enfrentar as ameaças cibernéticas e recomendam as melhores práticas para construir resiliência.
- O Centro de Cibersegurança do WEF defende a cooperação global e oferece recursos e fóruns para que as organizações possam partilhar conhecimentos e estratégias sobre resiliência cibernética.

A nova Diretiva Europeia sobre Segurança de Redes e Sistemas de Informação 2 (NIS2) deverá entrar em vigor já em outubro de 2024. A BDO desenvolveu uma ferramenta clara de avaliação NIS2 que pode fornecer-lhe informações imediatas sobre a sua situação atual. Pode aceder a esta ferramenta através do botão abaixo.

WWW.NIS2SURE.COM



Estratégias para aumentar a resiliência cibernética

Para fechar a crescente lacuna, existem várias medidas proativas que as organizações podem adotar, como:

01

Desenvolver um plano

Criar um plano abrangente que delineie medidas preventivas, protocolos de resposta a incidentes e estratégias de recuperação. Garantir que o plano esteja alinhado com a estratégia e os objetivos do negócio; rever e atualizar regularmente para refletir a evolução do ciberespaço e das necessidades empresariais.

02

Investir em tecnologia cibernética

Investir em tecnologia cibernética — como gestão da superfície de ataque e postura, controlos de segurança de dados, inteligência artificial focada na segurança e aprendizagem automática — que seja adequada, escalável, resiliente e segura, permitindo à organização detetar, responder e recuperar de ameaças e incidentes cibernéticos, ao mesmo tempo que oferece aos recursos mais valiosos a possibilidade de se focarem e automatizarem certas tarefas.

03

Fomentar uma cultura de ciberconsciência

Incentivar uma cultura em que a cibersegurança é uma responsabilidade partilhada, empoderando todos os níveis da organização.

04

Realizar formações regulares

Educar os colaboradores sobre as melhores práticas de cibersegurança e a importância do seu papel na manutenção da resiliência cibernética. 95% dos ciberataques são devido a erro humano, enfatizando a enorme necessidade de aprendizagem e desenvolvimento internos, em todos os níveis.

05

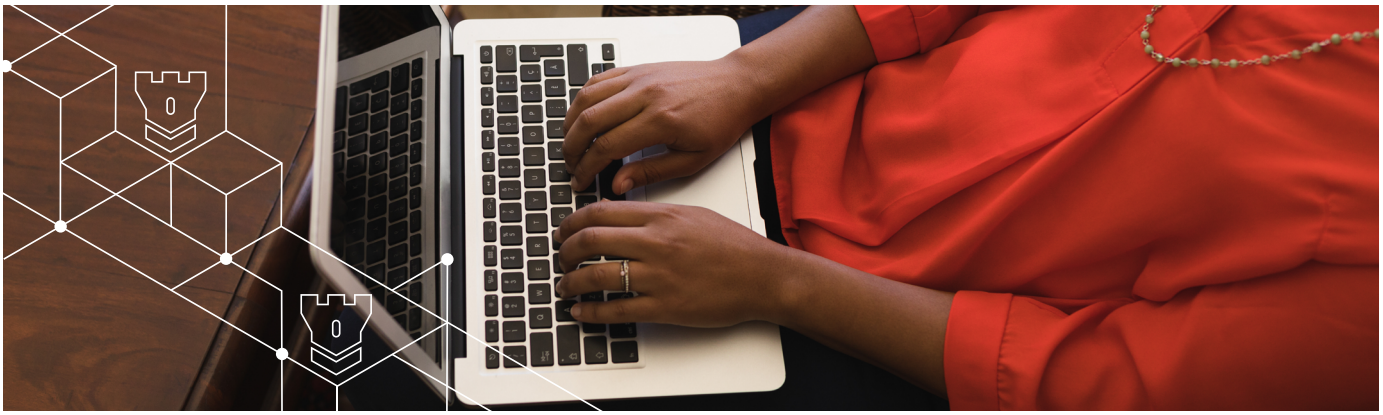
Estabelecer governança cibernética

Estabelecer uma governança cibernética que defina os papéis, responsabilidades e obrigações do conselho de administração, da gestão e da equipa, e que forneça políticas, normas e procedimentos claros e consistentes para a gestão de riscos cibernéticos e monitorização da conformidade, reporting e ações.

06

Realizar auditorias e avaliações regulares

Avaliar continuamente as medidas de cibersegurança e as estratégias de resiliência para identificar e abordar vulnerabilidades.



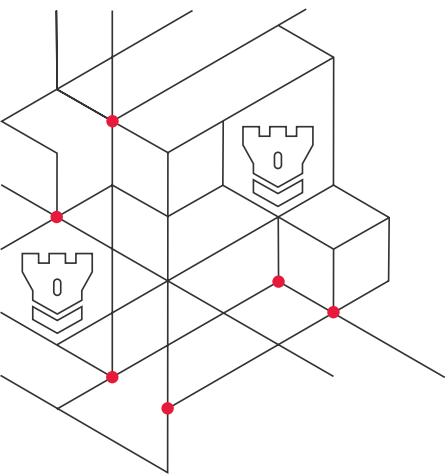
Conclusão

A crescente lacuna entre as organizações que são resilientes em cibersegurança e as que não o são sublinha a necessidade urgente de priorizar e incluir a resiliência cibernética como um objetivo empresarial fundamental. Ao compreender a sua importância, aproveitar perspetivas globais e implementar medidas estratégicas, as organizações podem salvaguardar os seus ativos, manter a continuidade operacional e construir confiança num mundo cada vez mais digital.

Cultivar as melhores práticas, atrair os talentos certos e implementar tecnologia personalizada ajudará a construir a resiliência necessária.

Já não se trata de saber se a sua organização estará em risco, mas sim de quando irá acontecer. Nenhum país ou organização estará a salvo do cibercrime, por isso é crucial que as partes interessadas globais trabalhem em conjunto para ajudar a fechar a lacuna.

À medida que as ameaças cibernéticas continuam a evoluir, também devem evoluir as nossas abordagens à resiliência, garantindo que estamos sempre um passo à frente no panorama da cibersegurança.



Como é que a BDO poderá ajudar?

Os fundamentos que os profissionais de cibersegurança implementaram estão a funcionar. A prática global de Cibersegurança da BDO é composta por profissionais de uma ampla gama de áreas, incluindo consultores experientes em TI, operações e privacidade de dados, bem como especialistas em tecnologia forense, consultoria empresarial e profissionais de contabilidade.

Estamos estruturados para fornecer serviços completos e personalizados a cada cliente, focados no seu modelo operacional específico, exigências técnicas, ambiente regulamentar e dinâmicas da indústria. Seja no setor de serviços financeiros, saúde, retalho, recursos naturais ou qualquer outro setor – entendemos as suas necessidades. A nossa presença global estende-se a todos os cantos do mundo, assim como o cibercrime. Deixe-nos ajudar a sua organização, onde quer que esteja, a mitigar os riscos cibernéticos que enfrenta.

Ricardo Moreira
Digital Director
BDO Portugal

8,4€ Biliões
custo do cibercrime em todo mundo em 2023

O custo global do cibercrime deverá aumentar para
21,3€ biliões em 2027,
em comparação com 7.7€ biliões em 2022 (Statista)

46%
participação das organizações que pagam resgates após um ataque de ransomware.

1,9 milhões
Número global de ameaças únicas reportadas por utilizadores finais em 2023.