bilingual edition

ptsoc {news}

17

Seguros de Ciber Riscos: quando a realidade aguça o engenho

3 perguntas a Pedro Figueiredo, Zurich Portugal

Gestão dos Riscos de Cibersegurança nas Organizações

.pt

Seguros de Ciber Riscos: quando a realidade aguça o engenho

A cobertura dos chamados Cyber Risks é relativamente recente na indústria seguradora. Tudo terá começado numa praia do Hawaii, em abril de 1997, durante a convenção anual da International Risk Insurance Management Society. Originalmente, a ideia consistia sobretudo em oferecer um produto capaz de proteger empresas cujos dados tivessem sido roubados dos seus servidores.

Quase três décadas passadas, o mundo das TI em 2025 é bastante diferente – e, sobretudo, bastante mais perigoso. De acordo com projeções recentes, o mercado de seguros de Cyber Risk deve chegar a 16,3 mil milhões de dólares em 2025 e subir para quase o dobro (30 mil milhões) até 2030.

Estes dados do mercado segurador acompanham de perto o aumento dos ataques e das perdas relacionadas com ciber-crimes, os quais dispararam para 9,5 biliões de dólares em 2024, um aumento significativo em relação aos 600 mil milhões registados em 2018.

Dados do Eurostat referentes a 2022 dão conta de que, em Portugal, apenas 10% das empresas possuem um seguro de Cyber Risks, valor que é metade do da média europeia e muito distante do país líder, a Dinamarca, onde 56% das empresas contrataram este tipo de coberturas.

Ransomware e Malware as a Service

Um dos tipos de ciberataque que mais tem crescido é o ransomware, que consiste na encriptação dos dados de uma empresa ou entidade, de forma a impedir o seu normal acesso, seguido de um pedido de resgate em troca da chave criptográfica que permita tornar esses dados novamente legíveis – daí o seu nome. O primeiro ransomware conhecido remonta a 1989 (anterior ao primeiro seguro de Cyber Risks), mas este tipo de ciberataque só se tornou mais comum a partir de 2016.

Segundo o mais recente relatório do Centro Nacional de Cibersegurança, o phishing continua a ser a ciberameaça mais comum em Portugal. Sendo esta uma técnica de engenharia social que tira frequentemente partido da distração, desconhecimento e/ou falta de formação dos funcionários das empresas e instituições é, igualmente, uma das formas mais usadas pelos cibercriminosos para injetar ransomware em equipamentos, redes e sistemas.

O panorama global da cibersegurança depara-se agora com mais um desafio: a utilização de ferramentas de IA de forma a aumentar a sofisticação e a facilidade dos ataques. De acordo com o World Economic Forum, "o aumento [dos ataques baseados em IA] (…) está a mudar o panorama da cibersegurança."

Além da sofisticação dos ataques – como é o caso dos chamados deepfakes – as ferramentas de IA também potenciam a utilização de "Malware as a Service" por parte de novos atores com menor sofisticação técnica e que, de outra forma, optariam por outro tipo de atividades criminosas. Um estudo recente da Europol considera mesmo os ciber-ataques como "o apogeu do 'Crime as a Service'".

PMEs e Conformidade

Na edição 15 da PTSOCnews, em que fizemos uma análise mais profunda do articulado da NIS2, identificámos já muitas das obrigações a que as entidades essenciais e as entidades importantes estão sujeitas em matéria de adoção de medidas rigorosas de segurança e, subsequente, reporte em tempo útil às autoridades competentes.

Mas desafiante é o facto de as micro, pequenas e médias empresas representarem 99,9% das empresas não-financeiras em Portugal – e estas, de acordo com um relatório recente da consultora Marsh, apresentarem controlos de cibersegurança, em média, 15% abaixo das grandes organizações, destacando-se, por exemplo, a menor implementação de estratégias de autenticação multifator. Além disso, de acordo com o mesmo estudo, apenas 40% das PMEs testam os planos de resposta a incidentes, versus 61% das grandes organizações.

Estas lacunas por parte das empresas são tanto mais graves quanto a diretiva NIS2 atribui à gestão das organizações responsabilidades diretas pela cibersegurança, nomeadamente através da exigência de supervisão, formação e alocação de recursos adequados para a implementação de práticas de segurança.

Neste contexto, importa lembrar que a gestão eficaz dos riscos de cibersegurança nas organizações requer a adoção de metodologias estruturadas que permitam identificar, avaliar e mitigar ameaças de forma sistemática.

Em Portugal, o Centro Nacional de Cibersegurança (CNCS) disponibiliza o Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança, o qual propõe uma abordagem baseada em normas internacionais como a ISO 31000 e a ISO/IEC 31010.

Também a nível europeu, a Agência da União Europeia para a Cibersegurança (ENISA) publicou o Compendium of Risk Management Frameworks with Potential Interoperability, documento que analisa diversas estruturas de gestão de riscos, incluindo as mencionadas anteriormente, e destaca a importância da interoperabilidade entre elas.

Os seguros de Cyber Risks

Os seguros de Cyber Risks (também em Portugal, o termo em inglês foi o que ficou consagrado pelas seguradoras) apesar de serem produtos de cobertura de risco, podem ter um papel importante em ajudar as empresas a estarem mais bem preparadas em termos

Foto: ImageFlow, adobe stock

de cibersegurança – além das coberturas de risco propriamente dito.

Isto porque, como referiu ao PTSOCNews João Lopes, da Guardian Seguros, "na maioria dos casos, na altura da subscrição destes seguros, existe uma análise por parte de empresas credenciadas para tal, onde se identifica a realidade da empresa, pontos de fragilidade e propostas de melhorias – informações que a grande maioria dos empresários em Portugal não tem em relação à sua empresa."

Além disso, estes são seguros que incluem quase sempre componentes de responsabilidade civil – crucial para qualquer empresa que detenha dados sobre clientes e fornecedores que possam de alguma forma virem a ser comprometidos – bem como capital para apoio jurídico e eventuais situações de ransomware.

"O mais importante", refere João Lopes, "é que a empresa possa rapidamente voltar à sua vida normal", uma vez que situações como as de um ataque de ransomware ou as de pedidos de indemnizações por perda de dados, envolvem frequentemente verbas significativas e, no caso de organizações com menores recursos, podem até obrigar ao encerramento da empresa.

Ao contrário de outro tipo de coberturas mais comuns, o cálculo dos prémios dos seguros de Cyber Risks não é simples. Ainda segundo João Lopes, "as tarifas têm em conta diversos fatores – desde o número e natureza dos equipamentos, a atividade desenvolvida, a dimensão da operação (número de clientes, número operações, etc…) e, uma vez que já começa a existir histórico, também a sinistralidade – quer do próprio cliente como do setor de atividade em que a empresa se insere."

3

Pedro Figueiredo

Head of Technical Underwriting da Zurich Portugal

1. Sabemos que as PMEs representam grande parte da economia e que cada investimento é ponderado. Este tipo de seguro é recomendado para qualquer empresa com presença digital, ou há exceções? Ou seja, um seguro de Cyber Risks faz mesmo sentido para todas as empresas, ou há casos em que não compensa?

Com a inovação tecnológica a impulsionar a digitalização da economia global, e com as empresas – independentemente do seu tamanho e setor de atividade – a dependerem cada vez mais das tecnologias digitais para o seu crescimento e inovação, os ciberriscos vão representar uma ameaça cada vez mais severa para as empresas. Prevê-se, aliás, que o custo global do cibercrime aumente cerca de três vezes entre 2022 e 2027 para quase 24 triliões de dólares.

Pequena ou Média não significa segura e são cada vez mais as empresas a reconhecer vulnerabilidade a este risco específico e a protegerem-se com seguros de Cyber Risks. Apesar disto, ainda são muitas as empresas, sobretudo as pequenas e médias, que correspondem a cerca de 98% do nosso tecido empresarial, que relegam esta proteção para segundo plano, mas que podem ser vistas pelos ciber-criminosos como alvos fáceis. É importante recordar que muitos ciberataques são, frequentemente, oportunísticos.

Por vezes, as PME debatem-se com dificuldades em compreender todos os riscos a que estão expostas e o nível de proteção que necessitam. Como tal, o mercado segurador deve contribuir com o desenvolvimento de soluções que simplifiquem o processo de subscrição destes seguros e possibilitem a cobertura de alguns desses riscos através de uma solução standard.

Neste sentido, uma vez que as ameaças digitais estão em constante evolução e ultrapassam a capacidade de resposta das soluções tradicionais de seguro e gestão de risco, o que é necessário são soluções inovadoras para mitigar as lacunas existentes entre o risco digital e a segurabilidade – principalmente para as PME – tal como

destacamos no whitepaper Closing the cyber risk protection gap, desenvolvido pelo Grupo Zurich e pela Marsh McLennan.

2. Que coberturas são essenciais num seguro de Cyber Risks para garantir proteção real e retorno sobre o investimento? O que deve uma empresa esperar e exigir de uma apólice para sentir que está verdadeiramente protegida?

O setor segurador é capaz de oferecer algum grau de proteção, e, por isso, como já foi sublinhado, é essencial que todas as empresas, dada a dependência crescente das tecnologias, se protejam com um seguro de Cyber Risks. Algumas coberturas que podem ser importantes são, por exemplo, a responsabilidade civil por danos causados a terceiros, a recuperação de dados por sequestro informático e a perda de lucros pela interrupção da atividade do segurado.

Há que reconhecer também que os cibereventos de grande escala apresentam riscos de acumulação substanciais – que não podem ser suportados pelo setor privado.

Neste sentido, a melhoria da resiliência cibernética das empresas e a adoção de mecanismos de controlo de segurança, que reflitam as melhores práticas de mitigação de riscos – por exemplo, de ransomware – deve ser uma prioridade. Para alcançar este objetivo, são necessárias, parcerias público-privadas sólidas, para desenvolver estratégias abrangentes que garantam o nosso futuro digital e a resiliência contra ciberameaças.

Afinal, é importante ter em conta que nem tudo pode ficar sob a alçada do seguro: há riscos cibernéticos não seguráveis, como a falha de infraestruturas críticas ou o pagamento de resgates. Assim sendo, para o que não seja malware em massa ou a interrupção em massa do acesso à cloud – incidentes cibernéticos, que, atualmente e até determinado nível de perda financeira, são considerados seguráveis – será uma parceria público-privada a resposta que pode garantir uma proteção eficaz.

O setor privado tem uma capacidade de financiamento limitada e, como conclui o whitepaper, para o fortalecimento da sociedade e da economia no caso de um evento cibernético catastrófico, é fundamental um maior envolvimento do setor público.

3. Como se calcula o valor a pagar por um seguro de Cyber Risks? Quais são os fatores mais relevantes — tamanho da empresa, área de atividade, infraestrutura tecnológica, histórico de incidentes?

Tal como um seguro de outro tipo, o cálculo do valor a pagar, por cada empresa, por um seguro de Cyber Risks, depende de vários fatores. Empresas maiores, com um maior volume de dados, e com um grau de dependência em relação a tecnologias

Foto: Kookkii, adobe stock

digitais mais elevado, poderão estar mais expostas a ataques cibernéticos ou ataques mais complexos, e, por isso, poderão enfrentar prémios mais elevados. O mesmo acontece com empresas com um histórico de ciberataques, uma vez que são vistas como mais suscetíveis a novos incidentes.

Por outro lado, estes valores podem ser atenuados quando as empresas demonstram boas práticas de higiene cibernética e investem na formação sobre estas matérias dos colaboradores.

A par destas variáveis, os seguradores utilizam modelos de avaliação de risco que combinam também dados do mercado e tendências de ameaças cibernéticas. Além disso, é sempre realizada uma análise personalizada para compreender as necessidades específicas de determinada empresa e ajustar a apólice de forma apropriada.

Finalmente, é importante destacar que o défice de proteção contra os riscos cibernéticos é uma questão importante que tem de ser resolvida – a ameaça de ciberataques representa, como já ficou claro, um risco significativo para a estabilidade social e económica. E, neste cenário, o cálculo do custo de um seguro não é apenas uma questão técnica ou financeira. Antes, reflete a necessidade de uma maior colaboração, com o desenvolvimento de soluções inovadoras, a educação e o incentivo dos compradores de seguros e o melhoramento do mercado de seguros cibernéticos – para que, mais uma vez, se salvaguarde a nossa economia e sociedade.

Gestão dos Riscos de Cibersegurança nas Organizações

A Associação DNS.PT tem disponível um curso destinado a criar as competências necessárias para que os participantes sejam capazes de salvaguardar a integridade da sua organização, identificando vulnerabilidades e planeando estratégias de mitigação em caso de ciberataque.

Intitulado Gestão dos Riscos de Cibersegurança nas Organizações, este curso online e gratuito distribui-se por quatro módulos com avaliação formativa, precedidos de um módulo introdutório e terminando num módulo de síntese e instruções de obtenção de certificado.

Com a crescente digitalização dos serviços e negócios, cresce o risco de ciberataque e de comprometimento das operações vitais das organizações. O curso aborda o processo de identificação, avaliação e tratamento de riscos de cibersegurança nas organizações.

Nos primeiros módulos, apresenta-se em detalhe o processo de análise e gestão de risco e, no último módulo, o formando terá de por à prova os seus conhecimentos respondendo a exercícios de aplicação.

Foto: Таніщна Коновал, adobe stock

Entre outras competências, os formandos poderão esperar, no final do curso, serem capazes de:

- Reconhecer as principais ameaças e ciberataques em Portugal;
- Distinguir os conceitos de Gestão do Risco de Cibersegurança e respetivo processo;
- Identificar cenários de riscos aplicáveis a diferentes tipos de ativos, com base em ameaças e vulnerabilidades;
- Reconhecer controlos de cibersegurança implementados;
- Avaliar riscos de forma sistémica, aplicar critérios de impacto e de probabilidade, e priorizar os riscos;
- Especificar opções de tratamento do risco;
- Identificar, avaliar e rever riscos de um cenário real (com um caso prático).

Destinatários

Este curso destina-se a todas as empresas e organizações. Pretende-se dotar as empresas de estratégias, métodos e técnicas de gestão dos riscos de cibersegurança, explorando as diferentes fases da gestão do risco, desde a identificação, avaliação e tratamento dos riscos, de forma a minimizar proativamente as vulnerabilidades existentes nas organizações.

Todas as pessoas podem inscrever-se neste curso, não existindo nenhum requisito quanto à escolaridade ou certificação anterior. No entanto, para ter uma experiência o mais positiva possível neste curso, os organizadores aconselham a que o participante já detenha conhecimentos básicos de cibersegurança.

A inscrição é gratuita, a partir de https://www.nau.edu.pt/pt/curso/gestao-dos-riscos-em-ciberseguranca-nas-organizacoes/ e após registo na plataforma NAU (também gratuito).

O curso tem uma duração de 10 horas, mas a partir do momento da inscrição, poderá ser realizado ao ritmo do estudante, de acordo com a sua disponibilidade. No final, e para obter o certificado, o participante terá de ter, no mínimo, 70% de respostas corretas no conjunto dos questionários.

O curso encontra-se disponível na plataforma NAU até 5 de junho de 2026.

Dois milhões de registos em .PT

No dia 9 de junho de 2025, o restaurante Bossa Tavira fez história ao registar bossatavira.pt – o registo número 2.000.000 no domínio .pt.

O .PT assinalou o momento com um comunicado oficial em que refere que "este número reflete o dinamismo da internet em Portugal e a crescente escolha pelo domínio .pt por empresas, organizações e pessoas."

"Alcançar os 2 milhões de domínios .pt é um testemunho do trabalho contínuo do .PT e dos seus parceiros para promover a internet em Portugal", afirma a propósito Luisa Ribeiro Lopes, Presidente do Conselho Diretivo do .PT. *"Este marco demonstra a vitalidade da nossa economia digital e a importância do .PT como um ponto de encontro online, onde a inovação e o crescimento económico se unem à garantia de um ambiente online cada vez mais seguro e de confiança."*

Além disso, foi também criado um website, www.2milhões.pt, onde se convida todos os que tenham um website no domínio .pt, a contarem a sua história.

Comissão publica orientações para os fornecedores de modelos de IA

A Comissão Europeia publicou no passado dia 18 de julho orientações para ajudar os fornecedores de modelos de IA de finalidade geral ("general purpose AI models") a cumprir as obrigações do Regulamento Inteligência Artificial, com início em 2 de agosto de 2025.

Estas orientações clarificam as obrigações, proporcionando segurança jurídica a todos os intervenientes em toda a cadeia de valor da IA, e complementam o Código de Boas Práticas para a IA de Finalidade Geral.

Henna Virkkunen, vice-presidente executiva responsável pela Soberania Tecnológica, Segurança e Democracia da União Europeia, declarou a propósito: «*com as orientações hoje apresentadas, a Comissão apoia a aplicação harmoniosa e eficaz do Regulamento Inteligência Artificial. Ao proporcionar segurança jurídica sobre o âmbito de aplicação das obrigações do Regulamento Inteligência Artificial para os fornecedores de IA de finalidade geral, estamos a ajudar os intervenientes no domínio da IA, desde as empresas em fase de arranque aos principais criadores, a inovar com confiança, assegurando simultaneamente que os seus modelos são seguros, transparentes e alinhados com os valores europeus.*»

Foto: Anwesha Dey, adobe stock

Relatório de mitigação de abuso de DNS

Em resposta aos requisitos reforçados da ICANN para 2024 sobre abuso de DNS, a DNS Research Federation (DNSRF) lançou uma nova iniciativa para avaliar a conformidade e o desempenho no mundo real.

Usando dados da plataforma DAP.LIVE, esta análise foca em como os registrars e registries estão a mitigar ameaças de phishing e malware de forma eficaz — e com que rapidez agem dentro de janelas de resposta críticas.

O relatório completo foi publicado no passado dia 3 de junho.

No More Ransom

O website "No More Ransom" é uma iniciativa da Unidade de Crime de Alta Tecnologia da Polícia dos Países Baixos e do European Cybercrime Centre (EC3) da Europol, com o apoio das empresas de cibersegurança Kaspersky e McAfee, que tem com o objetivo de ajudar as vítimas de ransomware a recuperar os seus ficheiros cifrados sem terem que pagar a criminosos. O Centro Nacional de Cibersegurança também é parceiro do projeto.

Uma vez que é muito mais fácil evitar as ameaças do que lutar contra elas assim que um sistema é infetado, o projeto também visa educar os utilizadores sobre como é que o ransomware funciona e quais as medidas que podem ser tomadas para uma prevenção efetiva.

Neste momento, o website aloja ferramentas capazes de decifrar ficheiros que tenham sido atacados por várias dezenas de tipos de ransomware.

2ª edição

Organização

.pt

CURSO

Cód. GRCO

Gestão dos Riscos de Cibersegurança nas Organizações

Salvaguarde a integridade da sua organização identificando vulnerabilidades e planeando estratégias de mitigação em caso de ciberataque.

Descrição

Com a crescente digitalização dos serviços e negócios, cresce o risco de ciberataque e de comprometimento das operações vitais das organizações.

O curso "Gestão dos Riscos de Cibersegurança nas organizações" aborda o processo de identificação, avaliação e tratamento de riscos de cibersegurança nas organizações.

Nos primeiros módulos, apresenta-se em detalhe o processo de análise e gestão de risco e, no último módulo, o formando terá de por à prova os seus conhecimentos respondendo a exercícios de aplicação.

Formato

- Duração: 10 horas
- Esforço: 10 horas
- Ritmo: Ao ritmo do estudante
- Idiomas: Português

O curso distribui-se por um módulo introdutório, quatro módulos teóricos com avaliação formativa e um módulo marcadamente prático. O curso termina com um módulo de síntese e instruções de obtenção de certificado.

Curso

Entre 04/06/25 e 05/06/26

Curso através da plataforma nau SEMPRE A APRENDER

Mais informações em www.pt.pt

Esta publicação é produzida pelo .PT

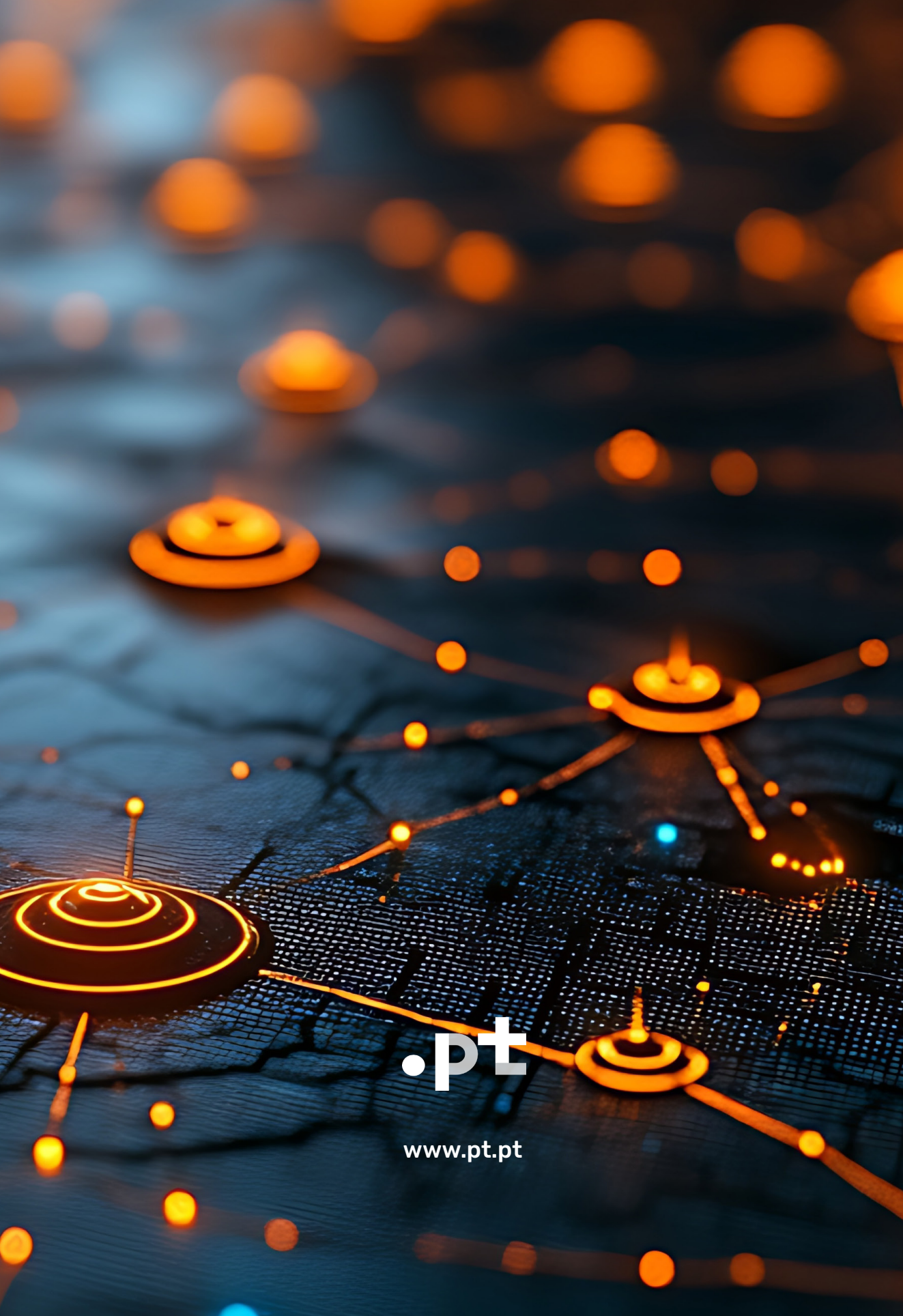
Editor
António Eduardo Marques

Design Gráfico
Sara Dias
Maria Cristóvão

Tradução
Sara Pereira

Fotografia
Capa: Nat, adobe stock
Índice e contracapa: yesdfg, adobe stock

Publicação trimestral
Julho 2025


.pt
www.pt.pt