devoteam
Cyber Trust

# **Tendências** em **cibersegurança** para **2025**

**Making your tech journey more secure**

# Quais as principais tendências de cibersegurança que devemos ter atenção em 2025?

## Introdução

### Com o final de 2024 e o aproximar de 2025, é tempo de refletir sobre os desafios enfrentados e o que nos reserva o futuro da cibersegurança.

Até agora, esta década trouxe-nos de tudo: ciberataques de alto risco, falhas tecnológicas de grande impacto e até uma pandemia global. Com este cenário em mente, olhar para 2025 implica contemplar as tendências emergentes e preparar-nos para o que está por vir.

O panorama da cibersegurança encontra-se atualmente numa fase de rápida transformação e são vários os fatores que contribuem para este contexto. As tensões políticas intensificaram-se, tornando os ciberataques patrocinados por estados-nação, uma preocupação global cada vez maior, assim como a crescente interdependência digital global, aumentando o impacto potencial desses ataques e transformando-os em ameaças que transcendem fronteiras.

Também, neste contexto de rápida mudança, a inteligência artificial (IA) fez avanços tecnológicos importantes, mudando radicalmente o cenário de ameaças e forçando as organizações a repensarem as suas estratégias de segurança. Isto levou a um **aumento do uso de ferramentas que utilizam IA e ML** (machine learning) para melhorar a deteção e resposta a ameaças.

Nos últimos anos, assistimos também a uma mudança nas táticas usadas pelos atores maliciosos. A crescente ênfase nas **abordagens baseadas em identidade** levou os profissionais de cibersegurança a reconsiderarem conceitos como "privilégio" e "segurança de identidade". A prioridade passou a ser a limitação do impacto de contas comprometidas, reforçando as defesas contra ataques baseados na identidade.

Com tanto por acontecer, **é essencial que as organizações se mantenham atentas às novas tendências** e ajustem as suas estratégias de segurança para enfrentar os desafios emergentes. Desta forma, tornou-se essencial encontrar soluções com abordagens simples e acessíveis a todos os colaboradores das organizações, que permitam passar de uma postura reativa de cibersegurança para uma postura proativa. Convidamos a explorar connosco o que irá redefinir o cenário da cibersegurança em 2025 e possivelmente nos anos seguintes.

devoteam
Cyber Trust

Para 2025 destacamos algumas tendências do ecossistema de cibersegurança:

# 1.

## O Realismo da IA

Em 2025, a inteligência artificial (IA) deverá ultrapassar a fase de expectativas inflacionadas e entrar numa etapa de maturidade, com as organizações a focarem-se em aplicações de valor concreto. A expansão dos agentes de IA autónomos será uma tendência chave, automatizando operações em áreas como segurança e logística, reduzindo tarefas manuais e melhorando a capacidade de resposta em atividades rotineiras. No entanto, este avanço trará novos desafios, exigindo estruturas rigorosas de governança para assegurar que as ações destes agentes respeitam as políticas e normas da organização, mitigando riscos éticos e de segurança. As Plataformas de Governança de IA irão assumir um papel essencial para garantir transparência e conformidade num cenário onde as exigências regulatórias variam.

A indústria adotará uma abordagem pragmática, prioritizando o impacto real da IA em contextos de alto valor operacional, com um foco reforçado em segurança e responsabilidade.

# 2.

## A Cibersegurança como Serviço (CaaS)

Espera-se que a cibersegurança como serviço (CaaS) cresça em popularidade à medida que as empresas procuram formas mais económicas de proteger os seus ativos digitais. A cibersegurança como serviço oferece às empresas soluções de cibersegurança externalizadas, que vão desde a monitorização contínua de ameaças até à resposta a incidentes. Ao utilizar estes serviços, até as empresas mais pequenas podem aceder a ferramentas de segurança avançadas sem necessidade de criar equipas internas.

As soluções de CaaS irão evoluir para incluir deteção de ameaças com IA, resposta a incidentes automatizada e análises em tempo real, que ajudarão as empresas a detetar e mitigar ameaças de forma mais rápida. À medida que os ciberataques se tornam mais sofisticados, a parceria com fornecedores especializados em cibersegurança oferecerá uma opção escalável e flexível para muitas organizações.

# 3.

## A Expansão da Arquitetura Zero Trust

O conceito de Arquitetura Zero Trust (ZTA), que opera com o princípio de "nunca confiar, sempre verificar", verá uma adoção generalizada. À medida que as ameaças cibernéticas se tornam mais avançadas, as organizações já não podem confiar na segurança baseada em perímetro. Em vez disso, a ZTA exige uma verificação contínua de utilizadores, dispositivos e aplicações — independentemente de estarem dentro ou fora da rede.

A expansão da ZTA ajudará a mitigar riscos como ameaças internas, movimento lateral numa rede comprometida e acesso não autorizado. Com mais organizações a mudarem para ambientes de cloud e trabalho remoto, a implementação da ZTA será crítica para manter uma segurança robusta e limitar potenciais brechas.

# 4.

## O Aumento do Roubo de Identidade Reverso

Em 2025, prevê-se um aumento significativo do **roubo de identidade reverso**, um fenómeno em que dados roubados ao longo dos anos são combinados de forma incorreta, resultando em "sósias digitais" que comprometem a verdadeira identidade das pessoas. Este problema pode surgir devido a falhas em bases de dados, onde a combinação de nomes comuns ou informações incorretas leva a reivindicações erradas ou até à troca de identidade, criando oportunidades para fraudes ou acusações injustas.

Com o crescente volume de dados pessoais expostos em múltiplas violações, a fusão incorreta de dados irá tornar-se uma preocupação crescente. Este tipo de roubo de identidade reverso poderá gerar impactos graves, desde problemas de crédito e disputas legais, até à criação de perfis digitais falsos usados para fins maliciosos. A prevenção exigirá uma vigilância maior sobre a integridade dos dados e a implementação de medidas rigorosas para verificar a identidade real de indivíduos.

# 5.

## A Cibersegurança Centrada no Ser Humano

O erro humano continua a ser um dos maiores riscos de cibersegurança, com ataques de phishing e palavras-passe fracas a representar uma parte significativa dos riscos. Desta forma, as organizações deverão ir além das formações tradicionais e adotar abordagens mais integrativas e contextuais, onde a consciencialização sobre segurança seja constantemente reforçada através de simulações realistas, micro formações e conteúdos adaptados ao comportamento e às funções específicas de cada colaborador.
Esta abordagem utiliza tecnologias como IA e análise comportamental para identificar potenciais riscos, direcionando o conteúdo certo, no momento certo. Além disso, práticas como a "gamificação" incentiva os colaboradores a adotarem práticas seguras de forma ativa e voluntária.

Outra tendência será o desenvolvimento de uma **cultura de cibersegurança**, onde a segurança se torne um valor organizacional partilhado e uma responsabilidade de todos, não apenas do departamento de TI. Tal significa adotar mecanismos simples, como o Alert Readiness Framework, no qual as organizações definem os seus próprios níveis de alerta adquiridos através de fontes de informação relevantes e qualificam cada uma delas, atribuindo-lhes um peso e, assim, as organizações conseguem calcular o seu nível de alerta atual. Aqui, os líderes e gestores terão um papel central em reforçar a importância do tema e criar um ambiente onde práticas seguras são constantemente promovidas e recompensadas. Em 2025, haverá um foco mais forte na cibersegurança centrada no ser humano, que enfatiza programas de formação e sensibilização para reduzir estas vulnerabilidades.

devoteam
Cyber Trust

# 6.

## As Mudanças Regulatórias e Conformidade

Com a rápida evolução das ameaças de cibersegurança, espera-se que os quadros regulatórios se tornem mais rigorosos até 2025. Os governos em todo o mundo estão a introduzir novas regulamentações que exigem que as organizações melhorem as suas práticas de segurança. Na União Europeia, a NIS 2 e o DORA são as normas que darão mais que fazer às instituições e empresas, exigindo uma adaptação robusta para garantir a resiliência digital, a proteção contra ciberameaças e a continuidade operacional. Enquanto a NIS 2 está a impor requisitos rigorosos de segurança cibernética e gestão de riscos, incluindo a proteção da cadeia de fornecimento e a resposta a incidentes, o DORA foca-se na resiliência operacional digital, cobrindo a segurança de TI, a recuperação de incidentes e monitorização contínua dos riscos, incluindo os de terceiros. Juntas, estas diretrizes forçam as organizações a fortalecerem as defesas cibernéticas, a implementarem práticas de governança mais rigorosas e prepararem-se para a recuperação rápida em caso de ataques, tudo isto com o objetivo de mitigar os riscos e assegurar a continuidade dos serviços críticos num ambiente digital cada vez mais complexo e dinâmico.

Além da NIS 2 e do Dora, o AI Act, aprovado em 2024, entrará também em vigor permitindo estabelecer a União Europeia como a referência mundial em matéria de regulamentação da IA.

# 7.

## Third-Party Risk Management Proativa e Colaborativa

A tendência dominante em 2025 para a gestão de riscos de terceiros (TPRM) no contexto da NIS 2 será a monitorização contínua e a avaliação automatizada de riscos ao longo de toda a cadeia de fornecimento. Com as exigências da NIS 2 a ampliar a responsabilidade das organizações sobre a segurança de terceiros, veremos uma maior adoção de ferramentas de inteligência artificial e machine learning para monitorizar em tempo reala postura de segurança de fornecedores e parceiros. O que permitirá identificar rapidamente vulnerabilidades ou comportamentos irregulares que possam indicar riscos.

Além disso, o mercado deve migrar para plataformas integradas de TPRM, que centralizam dados de riscos e facilitam auditorias e conformidade com a NIS 2, permitindo às empresas demonstrar de maneira mais eficiente o compromisso com a segurança cibernética ao longo de toda a cadeia. A exigência de resposta rápida a incidentes incentivará as organizações a manter canais de comunicação ágeis e transparentes com os fornecedores, além de estabelecer protocolos de resposta conjunta em caso de incidentes. Dessa forma, a TPRM em 2025 será cada vez mais proativa e colaborativa, fundamentada na automação e na transparência para lidar com os desafios impostos pela NIS 2.

# 8.

## Desafio na Retenção e Captação de Talento

Este é um tema que se irá manter em 2025. A captação e retenção de talento em cibersegurança enfrenta desafios significativos, impulsionados pela **crescente procura por profissionais qualificados e pela rápida evolução das ameaças digitais**. A velocidade com que as novas tecnologias e tipos de ataques surgem exige que estes profissionais estejam sempre atualizados, o que torna o mercado altamente competitivo e torna a retenção um desafio para as empresas. Além disso, a escassez de talentos em cibersegurança faz com que os profissionais mais qualificados sejam frequentemente disputados.

Outro desafio é o **desgaste psicológico da área**, já que os especialistas em cibersegurança lidam com alta pressão para proteger dados sensíveis e responder rapidamente a ameaças. A carga emocional pode levar ao esgotamento e à rotatividade de pessoal. Para lidar com esses desafios, muitas organizações irão continuar a investir em formação contínua, benefícios que promovem o bem-estar e ambientes de trabalho flexíveis, além de criar uma cultura de suporte e colaboração, essenciais para manter esses talentos no longo prazo.

# 9.

## A Melhoria das Estratégias de Defesa e Recuperação Contra Ransomware

Os ataques de ransomware continuam a evoluir, tornando-se mais sofisticados e difíceis de defender. As empresas devem concentrar-se tanto na prevenção destes ataques, como na criação de estratégias robustas de recuperação. Cópias de segurança regulares, redes segmentadas e o uso de soluções de Deteção e Resposta a Endpoints (EDR) serão componentes-chave de uma defesa forte contra ransomware.

À medida que as táticas de ransomware se tornam mais agressivas, como a dupla extorsão (exigindo resgates tanto para as chaves de desencriptação, como para a não divulgação de dados roubados), as empresas também terão de investir em seguros de cibersegurança e planos de resposta para minimizar interrupções operacionais.

No último ano, o panorama da cibersegurança revelou desafios significativos, impulsionados pela sofisticação de ameaças baseadas em inteligência artificial (IA), pela evolução dos ataques de ransomware e pela necessidade de fortalecer as cadeias de confiança de identidade. **A IA democratizou o hacking**, permitindo que até atacantes pouco experientes criassem campanhas de phishing e malware altamente complexos, desafiando os sistemas de deteção tradicionais. Além disso, grupos organizados têm analisado infraestruturas de rede em detalhe, explorando vulnerabilidades e vendendo acessos a terceiros em mercados ilegais, expondo as organizações a um aumento substancial dos riscos.

Em 2024, as cadeias de confiança de identidade tornaram-se um alvo crítico. **Métodos convencionais**, como a autenticação multifator, **mostraram-se insuficientes para mitigar ataques avançados** que exploram tokens de sessão e chaves de API. Estes incidentes evidenciam a necessidade urgente de implementar estratégias de segurança mais robustas, como verificações contínuas, gestão dinâmica de identidades e uma abordagem baseada em Zero Trust, capaz de reduzir a superfície de ataque e reforçar a resiliência.

À medida que 2025 se aproxima, **espera-se que as ameaças evoluam rapidamente em termos de sofisticação**, com ataques cada vez mais direcionados, imprevisíveis e difíceis de mitigar. Técnicas como automação avançada e randomização de malware aumentarão a complexidade dos ataques, enquanto a IA permitirá aos cibercriminosos personalizar campanhas em larga escala e explorar vulnerabilidades em cadeias de fornecimento e sistemas interconectados. Para enfrentar este cenário, as organizações devem adotar práticas como testes de intrusão orientados por ameaças (TLPT) e Red Teaming, que simulam cenários reais para identificar e corrigir lacunas antes que sejam exploradas. Estas práticas, complementadas por auditorias regulares, simulações de incidentes e soluções avançadas como autenticação contínua e monitorização comportamental, são essenciais para proteger ativos críticos e reforçar a preparação das equipas de segurança.

**O verdadeiro diferencial em 2025 será** a prontidão, no concreto **a ciberprontidão**, definida pela capacidade das organizações de antecipar, detetar e responder de forma eficaz às ameaças. Esta abordagem integrada, que une tecnologia, processos e pessoas, será essencial para fortalecer a resiliência, garantir a continuidade operacional e consolidar a confiança num ambiente digital cada vez mais complexo e desafiador.

## Bibliografia

https://www.forrester.com/blogs/predictions-2025-cybersecurity-risk-privacy/

https://www.park.edu/blog/cybersecurity-trends-protecting-business-information-in-2025/

https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

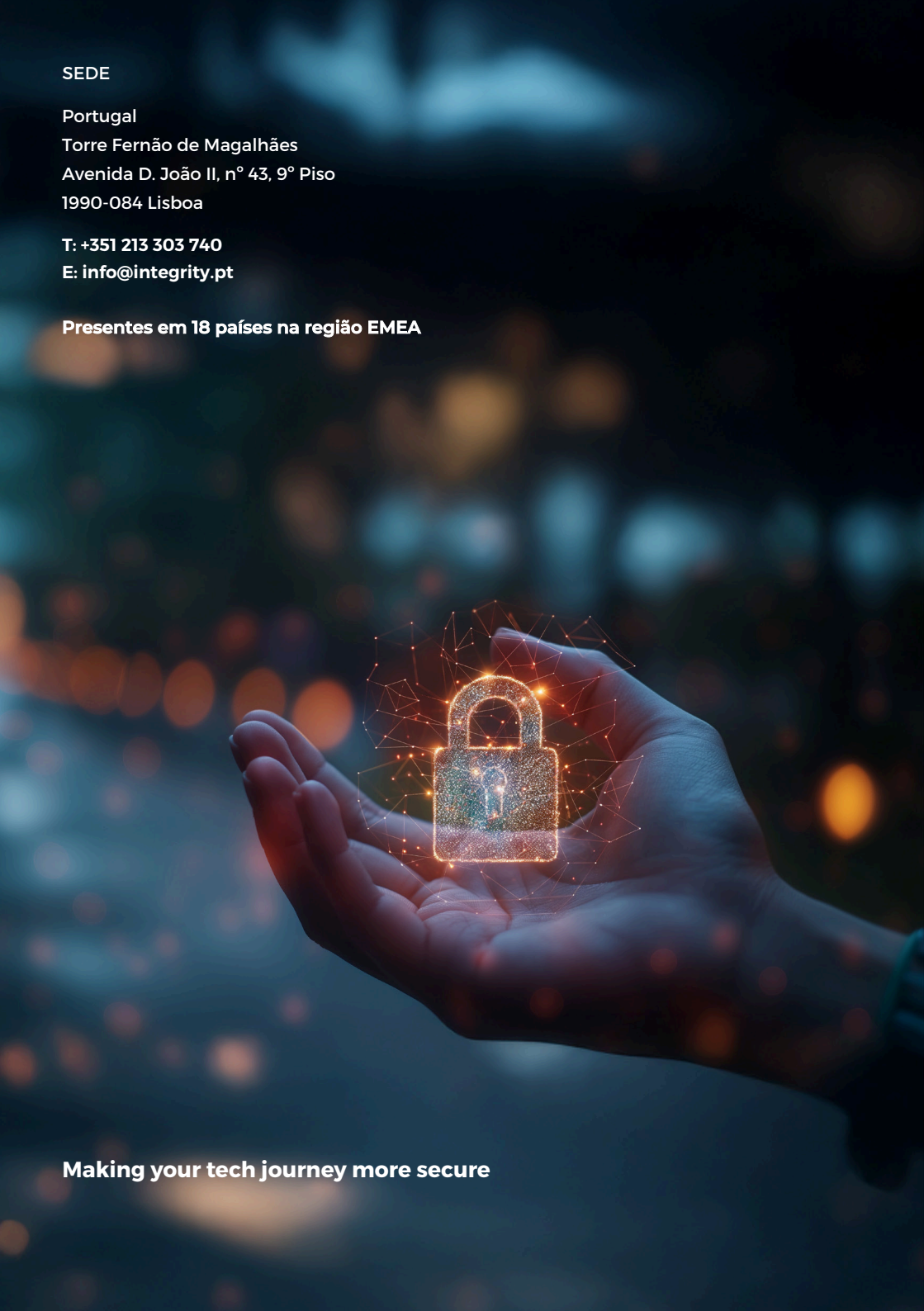
https://www.uscsinstitute.org/cybersecurity-insights/resources/top-cybersecurity-trends-to-watch-out-for-in-2025

SEDE

Portugal
Torre Fernão de Magalhães
Avenida D. João II, nº 43, 9º Piso
1990-084 Lisboa

**T: +351 213 303 740**
**E: info@integrity.pt**

**Presentes em 18 países na região EMEA**



**Making your tech journey more secure**