As 10 Tendências que vão redefinir a Cibersegurança em 2026 segundo a Devoteam Cyber Trust

Lisboa, 03 de dezembro de 2025 — A **Devoteam Cyber Trust** reuniu num relatório as **10 Tendências de Cibersegurança para 2026**, resultando num guia essencial para proteger indivíduos e organizações, num contexto cada vez mais digital, automatizado e global, onde destaca os desafios emergentes e as melhores práticas para **antecipar ameaças, gerir riscos e fortalecer a resiliência cibernética.**

O ano de 2026 promete ser um marco na evolução da cibersegurança, impulsionado por uma transformação digital cada vez mais acelerada e por um cenário de ameaças em constante mutação. A convergência entre inteligência artificial, computação quântica e conectividade global está a criar novas oportunidades, mas também vulnerabilidades inéditas. A cibersegurança afirma-se, assim, como um pilar estratégico de competitividade e confiança, pelo que **antecipar as tendências emergentes será fundamental para enfrentar os riscos do futuro digital com eficácia, ética e visão**.

Segundo Hugo Mestre, Executive Director & Head of Devoteam Cyber Trust Portugal, *"a trajetória para 2026 consolida a Cibersegurança como o motor da Confiança Digital. O desafio decisivo passa agora por harmonizar a aceleração da IA e o risco pós-quântico com um controlo rigoroso da identidade e da exposição. É esta capacidade de governar uma superfície de ataque em permanente evolução que representa a verdadeira prova de resiliência, convertendo a segurança no alicerce estratégico para dominar a complexidade e preparar o futuro".*

Conheça as **10 Tendências de Cibersegurança da Devoteam Cyber Trust:**

1. IA em Todo o Lado: Segurança à Velocidade da Máquina

A IA passa a estar integrada em quase todas as camadas da segurança: deteção de anomalias, apoio ao SOC, automatização de resposta e análise de grandes volumes de dados. Em paralelo, atacantes usam IA para criar campanhas de fraude mais credíveis, deepfakes e intrusões com maior rapidez. A tendência não é apenas usar IA na segurança, mas sim governar e proteger a própria IA, incluindo modelos, dados e decisões, como um novo ativo crítico da organização.

2. Início da Transição para Criptografia Pós-Quântica

O risco de recolher dados cifrados para os tentar decifrar no futuro leva as organizações a preparar-se para a era quântica antes de esta chegar em força. Em

2026, ganha tração o inventário dos mecanismos de cifragem, a identificação de sistemas sensíveis a longo prazo e a definição de roteiros para adoção de algoritmos pós-quânticos. A grande mudança está em tratar a criptografia como algo dinâmico e gerível, e não como uma decisão feita uma vez e esquecida.

3. Zero Trust Operacional em Ambientes Híbridos e Multicloud

O Zero Trust deixa de ser uma visão abstrata e passa a ser um programa de transformação visível na forma como o acesso é desenhado e controlado. Em 2026, redes e aplicações passam a ser segmentadas em função de sistemas críticos, as VPN tradicionais com acesso alargado são substituídas por modelos de acesso condicionado à identidade, ao contexto e ao dispositivo, e as políticas de acesso tornam-se consistentes em datacenter, cloud e SaaS. O impacto é direto: ambientes mais contidos, menor raio de impacto de incidentes e decisões de acesso alinhadas com os fluxos de negócio.

4. CTEM como Linguagem Corrente de Exposição ao Risco

A gestão contínua da exposição (CTEM) substitui relatórios pontuais de vulnerabilidades por uma visão viva do risco. As organizações passam a combinar vulnerabilidades, configurações, acessos, terceiros e processos numa mesma matriz de exposição. A tendência de 2026 é usar CTEM não apenas como ferramenta técnica, mas como linguagem comum entre segurança, risco e negócio para decidir o que corrigir, quando e porquê.

5. Identidade e Comportamento como Plano Principal de Controlo

A identidade deixa de ser apenas o login e passa a ser o plano onde se exerce a maior parte dos controlos de segurança. Em 2026, a mudança está em tratar identidades, sessões e comportamentos como um sistema operativo transversal: tudo o que importa, incluindo aplicações, dados e cloud, é governado por políticas de identidade e por análise de uso real. A novidade não está no phishing em si, mas na forma como a identidade passa a ser gerida com métricas, revisão contínua de privilégios e deteção de utilização anómala como indicadores centrais de risco.

6. Cloud, Dados e Cadeia de Software como Superfície Única de Ataque

Cloud, dados e cadeia de software deixam de ser três temas separados. Plataformas de proteção cloud, inventários de componentes (SBOM) e soluções de gestão da postura de segurança de dados convergem para uma visão única da superfície de ataque digital. A tendência de 2026 é olhar para código, infraestrutura e dados como partes do mesmo problema: saber exatamente o que corre onde, quem desenvolveu, de que depende e que informação sensível está em jogo.

7. Industrialização do Cibercrime, RaaS e Democratização do Alvo

O crime digital organiza-se em cadeia de valor: quem vende acessos, quem desenvolve malware, quem faz extorsão, quem trata da lavagem de fundos e quem oferece ransomware-as-a-Service como produto pronto a usar. Esta industrialização reduz drasticamente o custo e a barreira de entrada para atacar. Em 2026, a

implicação chave é que mais organizações, incluindo as de menor dimensão, passam a ser alvos economicamente interessantes, porque o esforço marginal para atacá-las é muito baixo. A resposta deixa de poder basear-se na ideia de que se é demasiado pequeno para interessar.

8. Regulação de Alto Impacto e Risco Expresso em Euros

NIS2, DORA e o enquadramento europeu de IA consolidam um novo patamar de exigência em cyber resiliência. A tendência não é apenas ter mais regras, mas ter mais escrutínio sobre evidência real de controlo e maior pressão para traduzir risco cibernético em impacto económico. Modelos de quantificação de risco que ligam falhas técnicas a perdas financeiras ganham espaço como ferramenta de decisão, colocando a segurança lado a lado com outros riscos estratégicos.

9. Convergência IT/OT e Soberania Digital como Fatores de Arquitetura

Os sistemas industriais, de saúde, energia e transporte estão cada vez mais ligados a redes IP e à cloud, aproximando as decisões tecnológicas das operações físicas. À medida que as TI e as TO começam a partilhar infraestruturas, fornecedores e serviços cloud, escolhas como residência dos dados, jurisdição aplicável e fabricantes de confiança deixam de ser detalhes técnicos para se tornarem decisões estruturais sobre soberania digital.

Crucialmente, esta convergência expande dramaticamente a superfície de ataque. Os arquitetos devem abordar de forma fundamental a segurança dos sistemas de tecnologia operacional (OT), que muitas vezes estavam isolados (air-gapped) ou foram concebidos sem protocolos de segurança robustos, através da implementação de controlos de segurança profundos, modelos de zero-trust e monitorização contínua desde a base.

10. Segurança Centrada nas Pessoas e Sustentabilidade Digital

A maior parte dos incidentes relevantes continua a depender de decisões humanas, e as equipas de segurança enfrentam níveis elevados de pressão e fadiga. Em 2026, ganha força uma abordagem de segurança centrada nas pessoas: processos, interfaces e incentivos são desenhados para reduzir erros prováveis e facilitar comportamentos seguros no dia a dia. Em paralelo, a sustentabilidade digital traduz-se em menos dados redundantes, sistemas mais simples e ciclos de vida bem geridos, reduzindo simultaneamente risco, custo e complexidade.

Com tanto por acontecer, **é essencial que as organizações se mantenham atentas às novas tendências e que ajustem as suas estratégias de segurança para enfrentar os desafios emergentes**. Desta forma, torna-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.**

Aceda à informação completa aqui:
https://www.integrity.pt/pt/landing/trends-2026.html

Sobre a Devoteam 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 do CIS - Centro de Segurança na Internet. Também somos acreditados pela Iniciativa Europeia de Pagamentos (EPI) para realizar avaliações de segurança do Wero, a carteira digital móvel. Com uma base considerável de clientes, operamos em mais de 20 países.

Contactos

BE Ideas | Boutique PR Agency
Sofia Alcobia
sofia.alcobia@beideas.pt

Magda Carvalho
magda.carvalho@beideas.pt