devoteam

Tendências de Cibersegurança 2026

Sobre a Devoteam

A Devoteam é uma empresa de consultoria premium que impulsiona negócios digitais e transformação por meio de tecnologia inovadora.

Com mais de 30 anos de experiência em tecnologia, oferecemos resultados duradouros em nuvem, dados, cibersegurança e IA para indústrias e instituições públicas em toda a região EMEA.

Na Devoteam, o empreendedorismo tecnológico está no centro dos nossos valores, promovendo o nosso espírito como empresa em constante aprendizagem. Dentro desta cultura, atraímos e formamos os melhores profissionais, criando uma elevada densidade de talentos entre os nossos 11 000 especialistas. As parcerias sólidas sempre estiveram no centro do nosso ADN, razão pela qual colaboramos estreitamente tanto com gigantes tecnológicos de renome como com startups inovadoras emergentes. Este ecossistema permite-nos fornecer soluções duradouras que ajudam os clientes a liderar os seus setores.

AI-driven tech consulting

Tendências de Cibersegurança 2026

Resumo

Introdução

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. Organizações e governos enfrentam o desafio de proteger infraestruturas críticas, dados sensíveis e cadeias de valor altamente interligadas. Neste contexto, a cibersegurança afirma-se 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.

TOP 10 Tendências

Tendência 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.

Tendência 2

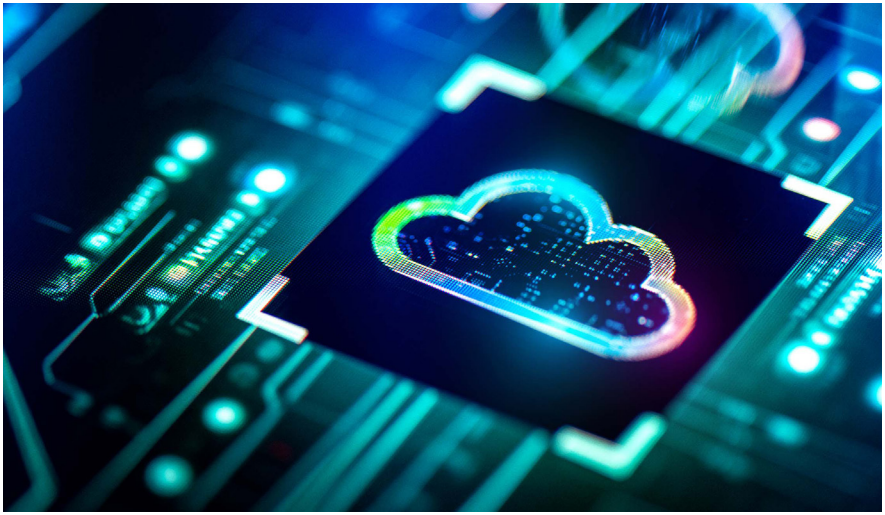
Início da Transição para Criptografia Pós-Quântica

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.

Tendência 3

Zero Trust Operacional em Ambientes Híbridos e Multicloud

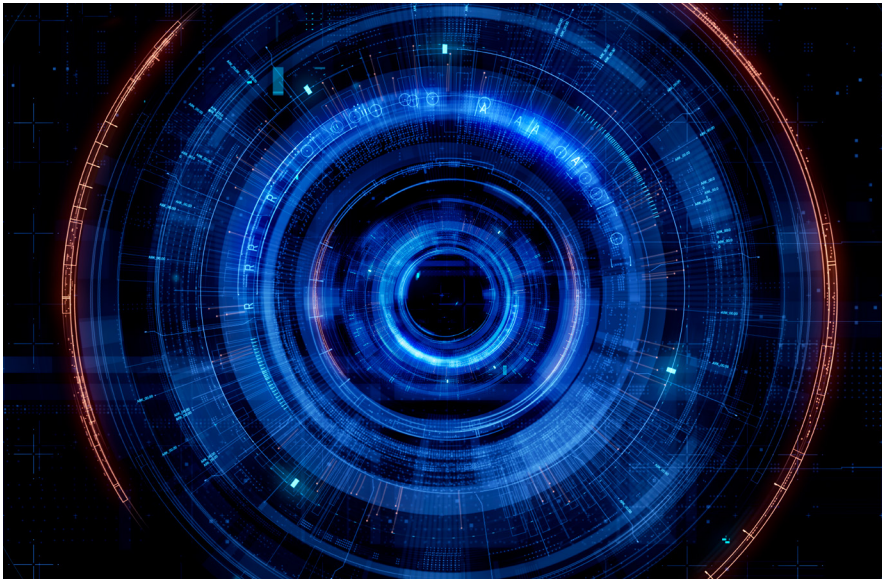
O Zero Trust deixa de ser uma visão abstrata e passa a ser um programa de transformação visível na forma como o acesso é desenhado e controlado. Em 2026, redes e aplicações passam a ser segmentadas em função de sistemas críticos, as VPN tradicionais com acesso alargado são substituídas por modelos de 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.



Tendência 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.



Tendência 5

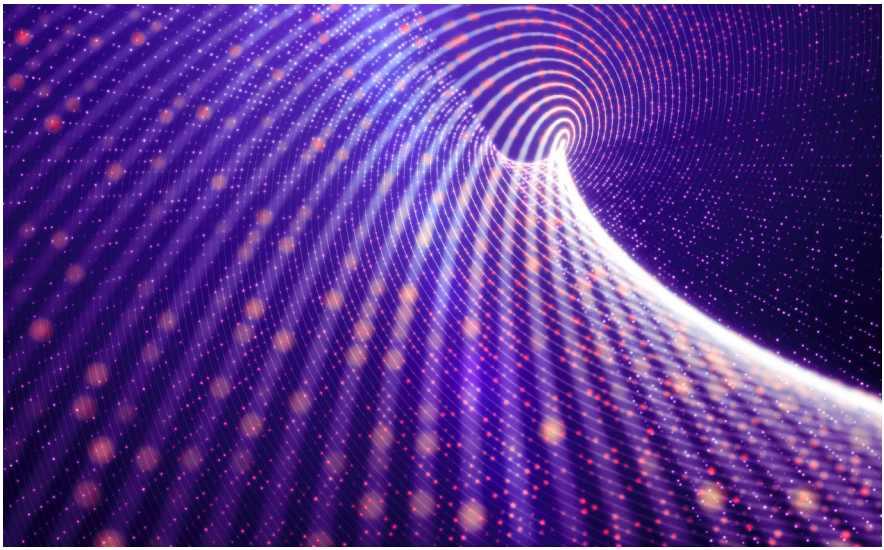
Identidade e Comportamento como Plano Principal de Controlo

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.

Tendência 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.



Tendência 7

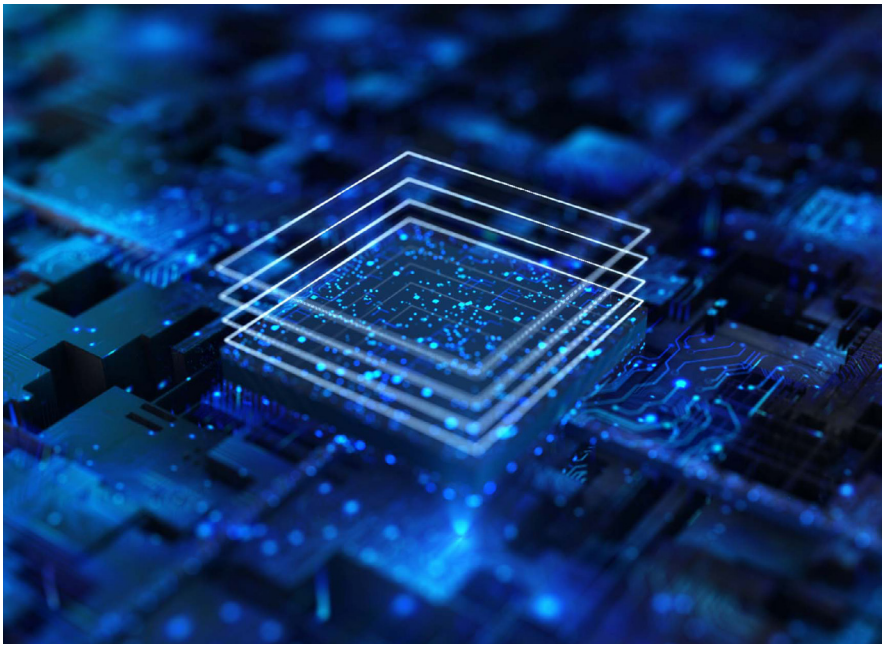
Industrialização do Cibercrime, Ransomware-as-a-Service e Democratização do Alvo

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.

Tendência 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 ciber-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.



Tendência 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.

Em 2026, as arquiteturas e as parcerias tecnológicas são concebidas não apenas com desempenho e custo em mente, mas também com resiliência face a ameaças ciberfísicas, dependências estratégicas e aos contextos regulatórios e geopolíticos em que as organizações operam.

Tendência 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.

Conclusão

Em 2026, a cibersegurança consolida-se como um elemento estratégico essencial para a sustentabilidade e competitividade das organizações. Num contexto marcado pela integração de tecnologias avançadas e pelo aumento das ameaças digitais, proteger dados, infraestruturas e operações deixou de ser opcional para se tornar um imperativo de gestão. A confiança digital será o alicerce das relações empresariais e institucionais, exigindo uma abordagem proativa, colaborativa e contínua para garantir resiliência e inovação segura.

Bibliografia

Gartner: The CIO's 2026 Cybersecurity Playbook
https://nationalcioreview.com/articles-insights/live-from-gartner-the-cios-2026-cybersecurity-playbook/

Top Strategic Technology Trends for 2026
https://www.gartner.com/en/articles/top-technology-trends-2026

Forrester forecasts agentic AI breaches & quantum spending surge by 2026
https://itbrief.asia/story/forrester-forecasts-agentic-ai-breaches-quantum-spending-surge-by-2026

ENISA Threat Landscape (ETL) 2025 report
https://www.iisf.ie/ENISA-Threat-Landscape-2025-report

CrowdStrike 2025 Ransomware Report: AI Attacks Are Outpacing Defenses
https://www.crowdstrike.com/en-us/press-releases/ransomware-report-ai-attacks-outpacing-defenses/

Cybersecurity in 2026: A Strategic Road Map for US Businesses
https://www.forvismazars.us/forsights/2025/10/cybersecurity-in-2026-a-strategic-road-map-for-us-businesses

NIST Post-Quantum Cryptography Standardization
https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization

2025 Identity Security Landscape Report
https://www.cyberark.com/threat-landscape

A Guide to CTEM
https://seemplicity.io/remops-glossary/ctem-continuous-threat-exposure-management/

Forrester's 2026 Cybersecurity and Risk Predictions
https://www.forrester.com/blogs/predictions-2026-cybersecurity-and-risk/

Google Cloud – Cybersecurity Forecast 2026
https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2026

AWS – Post-Quantum Cryptography Migration Plan
https://aws.amazon.com/pt/blogs/security/aws-post-quantum-cryptography-migration-plan/

BeyondTrust – Top Cybersecurity Predictions for 2026
https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions

Center for Internet Security – CIS Cyber Predictions 2026
https://www.cisecurity.org/insights/blog/7-cis-experts-2026-cybersecurity-predictions

Dúvidas?

Entre em contacto!

Em que ponto está da sua Jornada de Cibersegurança?

Vamos descobrir.
Estamos aqui para ajudar.

AI-driven tech consulting

devoteam.ai