

PROTEÇÃO DE DADOS

10 previsões para 2025

Das inovações tecnológicas às mudanças regulatórias, sem esquecer as pessoas: prepare a sua organização hoje para os desafios de segurança e conformidade de amanhã.

Quidgest



ÍNDICE

- 3 Editorial: A pergunta que não pode calar
- 4 Evolução contínua da regulação
- 6 Auditorias e penalizações mais severas
- 8 Impacto da IA e de outras tecnologias emergentes
- 10 Dados sensíveis e o desafio da monitorização
- 12 Novas ameaças de cibersegurança
- 14 Proteção em ambientes de trabalho híbridos e remotos
- 16 Segurança na nuvem e em servidores externos
- 18 Transferência de dados e padrões de privacidade
- 20 Avanços na autenticação e verificação de identidade
- 22 Pressão do cidadão/consumidor por mais transparência e proteção
- 24 Conclusão: E no final, tal como no princípio, as pessoas
- 25 Solução de Gestão de Proteção de Dados





A pergunta que não pode calar

Aproveitando a celebração do Dia Europeu da Proteção de Dados a 28 de janeiro, data criada para aumentar a consciencialização sobre a importância da privacidade e da segurança dos dados, convido todos os leitores deste e-book a refletirem sobre a resposta a esta pergunta: “Se amanhã fosse realizada uma auditoria de proteção de dados, a sua organização estaria totalmente preparada para garantir a conformidade com todas as exigências atuais?”

A crescente pressão pela conformidade, tanto a nível nacional quanto internacional, coloca as organizações numa posição de hipervigilância constante. Legislações como o Regulamento Geral de Proteção de Dados (RGPD) e outras normativas para a inteligência artificial ou a cibersegurança exigem adaptação contínua das práticas de segurança e transparência. O aumento das penalizações por falhas de conformidade – exemplificado por multas pesadas em empresas de diversas dimensões e áreas de atuação – reflete a intensificação das fiscalizações e a necessidade das organizações estarem devidamente preparadas.

Acompanhar e compreender os desafios da proteção de dados é o primeiro passo para evitar penalizações e manter a confiança dos cidadãos e consumidores. Tópicos como a proteção de dados sensíveis, o impacto da IA e outras tecnologias emergentes na gestão de dados, a segurança em ambientes híbridos e remotos, e a privacidade na nuvem vão ser temas centrais em 2025. E as organizações que não se adaptarem rapidamente podem arriscar a sua reputação e competitividade.

Neste e-book, abordamos 10 (quase 11) das principais tendências que estão a transformar o futuro da proteção de dados. O nosso objetivo é ajudar as organizações a anteciparem as mudanças tecnológicas e regulatórias em curso. Queremos também lembrar que a Quidgest dispõe de soluções digitais para a gestão da proteção de dados e a mitigação de riscos na segurança da informação. Estas ferramentas foram desenhadas para facilitar a adaptação às novas exigências e proporcionam maior agilidade e robustez na implementação de práticas de conformidade.

Assim, quando chegar o tal dia da auditoria que mencionamos no início deste editorial, a sua organização vai estar totalmente preparada para assegurar que todos os requisitos são cumpridos com total confiança.



Beatriz Bagoín Guimarães

Coordenadora do Departamento de Sistemas de Gestão de Informação e Processos de Negócio na Quidgest
IAPP CIPP/E

01

Evolução contínua da regulação

As regulações de proteção de dados desempenham um papel muito importante no avanço digital, ao estabelecerem padrões que garantem a segurança e a transparência num mundo cada vez mais movido a dados.





O RGPD tornou-se uma referência global, que tem vindo a influenciar legislações em diversas partes do mundo. Na China, a Personal Information Protection Law (PIPL) estabelece regras rigorosas para a gestão de dados pessoais e, nos EUA, a California Consumer Privacy Act (CCPA) concede aos consumidores um maior controlo sobre os seus dados pessoais. Estes são apenas dois exemplos de como diferentes jurisdições estão a adaptar as suas próprias regulações para responder a desafios locais.

Em 2023, a União Europeia avançou também com o [Data Governance Act](#), uma legislação que regula dados não pessoais e procura aumentar a partilha de dados de forma ética e segura. Paralelamente, nos EUA, foi apresentado um projeto de lei para uniformizar os padrões de privacidade entre estados, o que revela um esforço crescente para harmonizar regras num contexto regulamentar muitas vezes divergente.

Também o [AI Act](#) que entrou em vigor a 1 de agosto de 2024 surge como uma resposta às questões emergentes em torno do uso da inteligência artificial e os seus impactos na privacidade e segurança de dados. Esta legislação procura garantir

que a IA seja usada de forma ética, transparente e segura, protegendo os direitos dos cidadãos num contexto de rápida evolução.

Esta diversidade de cenários reflete não apenas os esforços globais para proteger os dados pessoais, mas também a necessidade de uma colaboração mais ampla. A Comissão Europeia, no seu [relatório de 2024](#) sobre a aplicação do RGPD, salientou que as grandes diferenças nos procedimentos administrativos nacionais e nas interpretações de conceitos no mecanismo de cooperação têm dificultado a harmonização na gestão de casos transfronteiriços em todo o espaço europeu. Esta falta de alinhamento nas regulações de proteção de dados pode resultar em processos mais demorados e complexos para a resolução de questões relacionadas com a segurança de dados pessoais.

À medida que a tecnologia avança e novos desafios surgem, a regulação vai também continuar a adaptar-se, de forma a garantir a segurança e a confiança no mundo digital. O objetivo é zelar por um espaço mais protegido e responsável para todos os seus utilizadores.

PRINCIPAIS DESAFIOS

As diferenças entre regulações complicam a conformidade internacional.

As novas tecnologias surgem mais depressa do que a legislação consegue acompanhar.

Muitos países carecem de agências capazes de monitorizar as aplicações locais.



O QUE ESPERAR DE 2025?

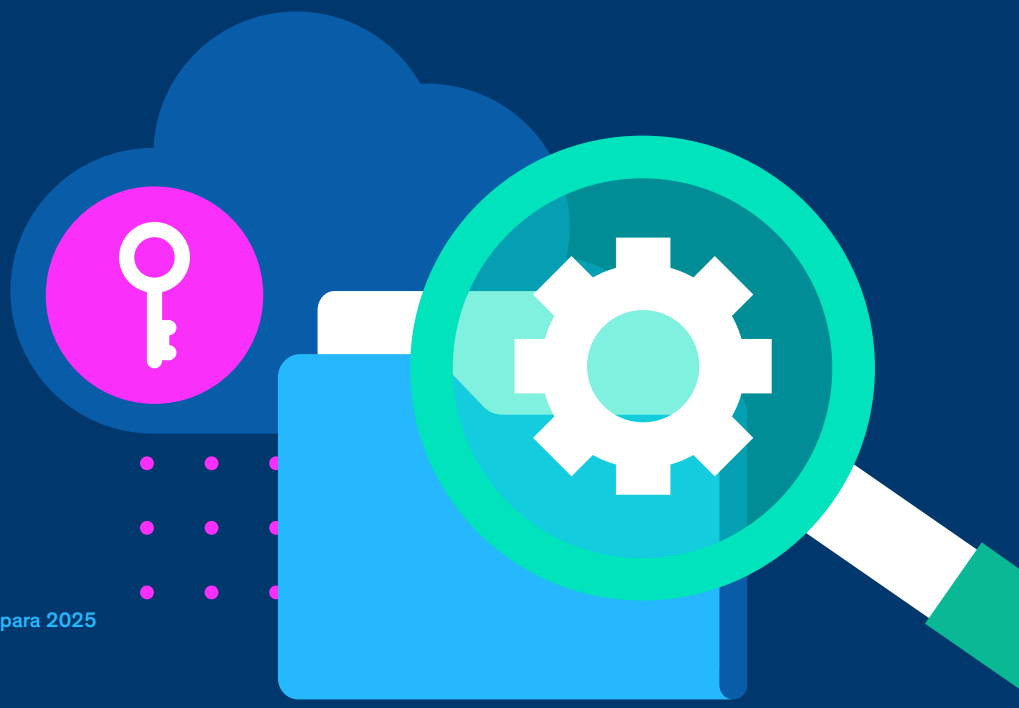
O futuro aponta para a criação de um ecossistema mais harmonioso, sustentado por uma colaboração entre órgãos reguladores, empresas e sociedade civil.

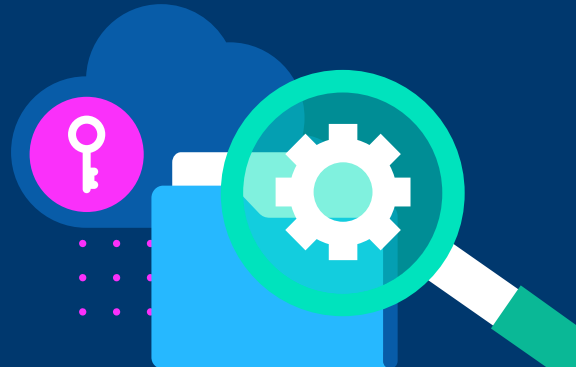
A legislação promete expandir-se para novos contextos, como a IA e os dados biométricos, mas também integrar-se de forma mais dinâmica com as inovações tecnológicas, antecipando desafios e garantindo uma proteção mais adaptada às realidades emergentes.

02

Auditorias e penalizações mais severas

Com a evolução da regulação, as auditorias e as penalizações tornaram-se ferramentas essenciais para garantir a conformidade das organizações com as leis de proteção de dados.





As autoridades reguladoras têm ampliado os seus poderes, aplicado multas severas e realizado fiscalizações mais frequentes. Estas medidas não têm como objetivo apenas punir as empresas em caso de falhas, mas também incentivar boas práticas de governação corporativa. O RGPD é uma das legislações que lidera este movimento, mas várias outras leis também reforçam a importância das auditorias e da conformidade.

Exemplos de empresas que sofreram as consequências da não conformidade incluem a British Airways (por um ciberataque que comprometeu os dados de 400 mil clientes) e a Amazon (práticas de publicidade que violaram as normas de consentimento) - enfrentaram multas de vários milhões de euros por falhas no cumprimento do RGPD. Na Austrália, o caso da operadora de telecomunicações Optus destacou também a vulnerabilidade dos dados (informações confidenciais como número de passaporte e dados financeiros de 10 milhões de pessoas foram expostas), o que resultou em auditorias obrigatórias e sanções financeiras que reforçaram a necessidade de proteção adequada da informação.

Outro caso emblemático de não conformidade deu-se na Equifax, nos EUA. Após uma fuga de dados que afetou 147 milhões de pessoas, a empresa teve de pagar mais de

700 milhões de dólares em multas e indemnizações. Na Ásia, a ZTE enfrentou críticas e penalizações por falhas na proteção de dados sensíveis dos seus clientes. Este caso alertou para os riscos associados à falta de segurança e à necessidade de práticas mais rigorosas de proteção de informações pessoais e comerciais.

As penalizações regulamentares vão continuar a ser rigorosas e a impactar profundamente a confiança dos stakeholders, a retenção de clientes, a reputação e a capacidade de inovação das organizações. Ou seja: o custo da não conformidade vai significar muito mais do que perdas financeiras.

Um [relatório da PwC](#) (2024) revela que, em média, 50% das empresas enfrentaram uma violação regulatória nos últimos cinco anos. Esta realidade sublinha o crescente desafio das organizações em garantirem a conformidade, especialmente à medida que novas regras e exigências entram em vigor. Paralelamente, um [estudo da Gartner](#) (2023) estima que o investimento em conformidade regulatória aumente 50% até ao final de 2026, o que mostra a importância crescente da regulação no panorama corporativo global.

PRINCIPAIS DESAFIOS

As auditorias exigem planeamento e mobilização de recursos financeiros e humanos.

As regras de auditoria tornaram-se mais detalhadas com a introdução de novas tecnologias.

As penalizações severas geram impactos negativos, além da multa, na reputação corporativa.



O QUE ESPERAR DE 2025?

As auditorias vão ser altamente automatizadas, com o uso de ferramentas baseadas em IA para a deteção de anomalias. Além disso, espera-se que as penalizações sejam mais frequentes em casos de negligência relacionados com dados sensíveis ou biométricos.

03

Impacto da IA e de outras tecnologias emergentes

A IA e outras tecnologias emergentes, como blockchain e Internet das Coisas, estão a revolucionar a forma como os dados são processados e protegidos.



03 | Impacto da IA e de outras tecnologias emergentes



Embora tais inovações estejam na origem de soluções que impactam positivamente a vida e os negócios, estas trazem consigo riscos para a segurança da informação – deep fakes, fake news, rastreamento de localização, aplicações de reconhecimento facial ou análise de comportamento online são frequentemente citados como exemplos de violação da privacidade que têm intensificado a aplicação de coimas e penalizações.

No entanto, são estas mesmas tecnologias que estão também a impulsionar o desenvolvimento de novas regulações e a tornar-se ferramentas importantes para melhorar as auditorias e ajudar as organizações a monitorizarem e corrigirem falhas de segurança de maneira mais eficaz e eficiente. Além de prevenirem fraudes e reforçarem a conformidade com as novas normas de privacidade, são capazes de automatizar a verificação de grandes volumes de dados, monitorizar transações em tempo real e otimizar a análise de riscos, proporcionando auditorias mais rápidas, precisas e eficazes.

Dada a complexidade e o impacto destas tecnologias, os reguladores começaram a avaliar como interagem com a proteção de dados, com foco em

áreas como algoritmos de decisão automatizada e biometria. Empresas como a Google e a Microsoft já adotaram abordagens responsáveis e desenvolveram diretrizes internas para mitigar riscos como o enviesamento algorítmico ou a falta de transparência. No entanto, casos como o da Clearview AI, que usou IA para reconhecimento facial sem consentimento adequado (foram recolhidas imagens de redes sociais e websites sem que os indivíduos fossem informados), exemplificam os perigos que surgem quando a tecnologia é utilizada à margem da lei.

Iniciativas como o AI Act da União Europeia têm como objetivo estruturar regulações que garantam o uso ético e seguro destas tecnologias. Nesta senda, um [estudo da McKinsey](#) (2023) refere que organizações de alto desempenho, provavelmente por estarem há mais tempo na jornada da IA, reconhecem com maior clareza os potenciais riscos associados (imprecisão, infrações de propriedade intelectual e questões de cibersegurança). Além disso, continua o relatório, 44% destas organizações integram já estratégias de proteção de dados e de mitigação de riscos desde as fases iniciais de desenvolvimento das suas soluções de AI, o que demonstra uma abordagem proativa e preventiva.

PRINCIPAIS DESAFIOS

Os algoritmos podem reproduzir preconceitos e desinformação existentes nos dados - áreas como saúde ou justiça exigem rigor ético redobrado.

Os utilizadores e os reguladores desconhecem, por vezes, como as decisões são tomadas através da IA.

Determinar quem é responsável por falhas algorítmicas ainda é um desafio.



O QUE ESPERAR DE 2025?

A regulação da IA deve avançar para incluir não apenas padrões de transparência, mas também frameworks específicos para cada setor. Além disso, o uso de IA para detetar e prevenir violações de privacidade vai, muito provavelmente, tornar-se uma prática comum, elevando a tecnologia ao patamar de aliada (e não apenas de prevaricadora) na proteção de dados.

04

Dados sensíveis e o desafio da monitorização

Dados sensíveis (como informações médicas, financeiras, biométricas, de localização, preferências de consumo, entre outras) exigem uma proteção reforçada devido aos riscos significativos associados ao seu uso indevido.



04 |

Dados sensíveis e o desafio da monitorização



Com a crescente quantidade de dados gerados por aplicações e dispositivos interconectados, monitorizar e proteger estas informações tornou-se um dos maiores desafios para organizações e governos.

Exemplo disto foi o ciberataque (do tipo ransomware) à rede norte-americana Universal Health Services, em 2020, no qual dados médicos, históricos de pacientes e informações de prescrição foram violados. O caso levantou a necessidade urgente de uma monitorização muito mais rigorosa. Em contrapartida, iniciativas como a criação de Data Trusts, no Reino Unido, têm surgido como uma resposta eficaz para proteger informações sensíveis, nomeadamente em projetos colaborativos que envolvem a partilha de dados. Estas estruturas asseguram que o controlo dos dados permanece nas mãos dos indivíduos, sem comprometer a privacidade ou os direitos dos titulares.

Em 2024, a Apple deu um passo significativo para reforçar a segurança dos dados de saúde dos seus utilizadores, ao implementar um sistema de criptografia avançada nos seus dispositivos. A tecnológica também intensificou as suas auditorias de segurança, realizou testes de

vulnerabilidade mais frequentes e utilizou IA para monitorizar os acessos não autorizados. Este trabalho proporcionou uma camada adicional de proteção contra ciberameaças. Também o sistema de pagamentos instantâneos Pix, no Brasil, foi alvo de críticas em 2024, após uma fuga de dados dos utilizadores que levantou questões sobre a eficácia das medidas de segurança do sistema. Em resposta, o Banco Central introduziu auditorias de segurança mais rigorosas, com o objetivo de monitorizar transações em tempo real e identificar comportamentos anómalos. Além disso, houve melhorias na criptografia dos dados e a autenticação multifator foi reforçada, garantindo mais segurança para os utilizadores.

O [relatório da IDC](#) (2024) projeta que, até ao final de 2025, quase 20% dos dados na esfera global passem a ser considerados críticos para o nosso dia a dia e que 10% desses possam vir a ser catalogados como hipercríticos. O mesmo estudo prevê que, até 2028, 80% dos CIO vão promover mudanças organizacionais para aproveitar a IA, a automação e a análise de dados, bem como estratégias eficazes para recolha de dados e prevenção de riscos associados à sua utilização indevida.

PRINCIPAIS DESAFIOS

A quantidade crescente de dados sensíveis dificulta a implementação de medidas de segurança em larga escala.

Os sistemas interconectados tornam mais desafiante garantir o acesso restrito e autorizado às informações sensíveis.

As diferentes regiões possuem critérios distintos para o tratamento e a proteção de dados sensíveis.



O QUE ESPERAR DE 2025?

A monitorização de dados sensíveis vai ser fortemente baseada em ferramentas de IA e blockchain, o que vai permitir elevados índices de rastreabilidade e segurança. Além disso, é provável que venham a ser criadas normativas de abrangência global para unificar a proteção de dados sensíveis, de forma a facilitar a conformidade a um nível internacional.

05

Novas ameaças de cibersegurança

A expansão digital global trouxe inovações e oportunidades, mas também abriu portas a uma crescente variedade de ciberameaças.





A [legislação NIS2](#), adotada pela União Europeia a 28 de novembro de 2022, é um marco regulatório para enfrentar estes desafios e exige às organizações de setores críticos como a saúde, a banca, a educação ou os transportes que adotem padrões de segurança mais rigorosos. No entanto, o cumprimento destas normas exige esforços significativos de adaptação não só tecnológica mas cultural.

No panorama global, a utilização de criptomoedas tem crescido de forma exponencial, o que as torna alvo preferencial para cibercriminosos. A sua natureza descentralizada e desregulada amplifica os riscos. Este cenário não se limita às criptomoedas, pois o mercado de jogos online, que superou os 150 mil milhões de dólares em 2023, também passou a ser terreno fértil para fraudes e atividades ilícitas, como a manipulação de resultados e a exploração de menores.

O financiamento de terrorismo tem sido outra preocupação, à medida que mais grupos extremistas se aproveitam da complexidade e do anonimato proporcionados pelo universo digital. Esta realidade tem impulsionado esforços globais para o fortalecimento das normativas. Exemplo disso são as diretivas contra o branqueamento de dinheiro da União Europeia, que estabelecem exigências rigorosas de

verificação da identidade dos clientes, no âmbito da luta contra o financiamento do terrorismo e a lavagem de dinheiro. Esta regulação abrange instituições financeiras reguladas e plataformas de criptomoedas, obrigando-as a aplicar processos de “Conheça o Seu Cliente” (KYC) e a realizar verificações rigorosas para impedir o uso destes sistemas para fins ilícitos.

Mas a evolução das ameaças digitais também se reflete num aumento de fraudes em transações eletrónicas. Um [estudo da PwC](#) (2023) revelou que este tipo de fraudes cresceu 28% em apenas dois anos, um claro sinal de que é urgente uma maior resiliência e colaboração internacional para antever, evitar e responder rapidamente a estes incidentes.

Ainda neste contexto, um [relatório da KPMG](#) (2023) destaca que, apesar da incerteza económica global, os líderes estão cada vez mais comprometidos com a transformação digital impulsionada pela adoção de tecnologias emergentes, como a IA, que tem gerado enormes ganhos de produtividade em vários domínios. No entanto, o relatório também aponta que a falta de coordenação entre os diferentes atores continua a ser um obstáculo

PRINCIPAIS DESAFIOS

Reforçar a resiliência organizacional com estratégias de prevenção, resposta e recuperação.

Otimizar os sistemas de deteção de ameaças, através de IA avançada e análise preditiva.

Fortalecer a segurança no processamento de dados sensíveis (banca, saúde, jogos online, exchanges de criptomoedas, entre outros).



O QUE ESPERAR DE 2025?

As ciberameaças vão continuar a evoluir, exigindo respostas cada vez mais dinâmicas e colaborativas. Tecnologias como a IA vão desempenhar um papel principal na identificação de padrões anómalos; e a NIS2 prepara-se para promover uma cultura de cibersegurança, tanto em ambientes corporativos como em plataformas de uso pessoal.

06

Proteção em ambientes de trabalho híbridos e remotos

Com a consolidação do teletrabalho, a proteção de dados passou a enfrentar novos desafios que ampliaram os riscos associados à segurança da informação.





A troca constante de dados, muitas vezes fora dos ambientes corporativos controlados, aumentou a exposição a ciberataques (phishing, ransomware, ataques de malware) e a variados riscos, como a vulnerabilidade de dispositivos pessoais ou o uso inadequado de redes Wi-Fi públicas. Além disso, o uso de redes domésticas em ambientes de trabalho ampliou a superfície de ataque, tornando difícil garantir que os sistemas de segurança se mantêm eficazes em todos os pontos de acesso. Isto exige que as organizações adotem medidas mais potentes, como criptografia, autenticação multifator e monitorização constante, para proteger as informações e garantir a conformidade com as regulações de privacidade.

Empresas como a Zoom e a Microsoft lideraram investimentos em tecnologias como a criptografia de ponta a ponta para proteger reuniões e dados partilhados em plataformas colaborativas. Paralelamente, foram introduzidas orientações específicas para mitigar os riscos no trabalho remoto – são disso exemplo as recomendações da European Union Agency for Cybersecurity (ENISA), que definem boas práticas de segurança em contexto europeu.

Há vários casos reais que ilustram a eficácia destas medidas. Durante a pandemia, o aumento de ataques ransomware levou o setor da saúde no

Reino Unido a adotar VPN reforçadas e políticas rigorosas de autenticação, o que ajudou a proteger dados sensíveis de pacientes mesmo em ambientes remotos. Já o Banco Santander implementou um programa de formação em cibersegurança, focado na consciencialização dos seus colaboradores sobre os riscos de comportamentos aparentemente inocentes, mas desastrosos (como clicar em e-mails suspeitos). A empresa realiza formações regulares, com simulação de ciberataques, para preparar os funcionários na identificação de tentativas de phishing e na adoção de práticas seguras (como autenticação multifator), protegendo assim dados sensíveis relacionados com operações do banco.

As medidas de segurança no trabalho à distância são tema de vários estudos. A [MIT Sloan](#) (2024) refere que uma das principais preocupações em ambientes de trabalho híbridos é a dificuldade de monitorizar e proteger dispositivos dispersos, devido ao risco de incidentes de segurança relacionados com a vulnerabilidade dos dispositivos não protegidos. Outro estudo da [Accenture](#) (2021) revelou que 83% dos colaboradores preferem trabalhar remotamente, mesmo reconhecendo os riscos adicionais de segurança. Estes dados destacam a necessidade de equilibrar flexibilidade e proteção no ambiente de trabalho atual.

PRINCIPAIS DESAFIOS

Muitos profissionais utilizam redes pessoais mais vulneráveis do que as redes corporativas.

A falta de conhecimento sobre cibersegurança é um risco significativo para as organizações.

As soluções de segurança nem sempre são compatíveis com diversas plataformas e dispositivos.



O QUE ESPERAR DE 2025?

As soluções de segurança zero trust vão tornar-se padrão e vão permitir verificar, continuamente, utilizadores e dispositivos. Além disso, as empresas vão passar a oferecer apoio técnico mais reforçado para proteger redes domésticas, o que poderá incluir a instalação de equipamentos de segurança personalizados.

07

Segurança na nuvem e em servidores externos

A migração de dados para cloud tornou-se uma tendência inevitável, impulsionada pela necessidade de mais flexibilidade, escalabilidade e eficiência. No entanto, a segurança deste ambiente permanece uma preocupação para empresas e utilizadores





À medida que a adoção de soluções baseadas na nuvem cresce, os fornecedores de serviços têm investido em tecnologias avançadas para proteger os dados contra acessos não autorizados (por indivíduos ou sistemas), violações (acesso, alteração ou divulgação indevida) e interrupções (ataques como DDoS, Distributed Denial of Service, ou falhas técnicas).

Exemplos desta evolução podem ser vistos em serviços como AWS, Azure ou Google Cloud, que proporcionam recursos avançados, incluindo criptografia por padrão, autenticação e monitorização contínua de ameaças. São ainda de mencionar regulações como o Cloud Act, nos EUA, e as diretrizes do RGPD, na União Europeia, que têm desempenhado um papel importante ao estabelecer padrões claros para a gestão e a proteção de dados na nuvem.

A par das soluções, encontramos desafios. Em 2023, a violação de dados da Capital One afetou mais de 100 milhões de utilizadores. Por causa de uma configuração inadequada na infraestrutura de nuvem, a falha permitiu que o atacante acesse a informações como dados de cartões de crédito e históricos de transações.

Este incidente destacou a necessidade de configurações rigorosas e práticas de segurança mais eficazes, como monitorização constante e autenticação multifator, para proteger dados sensíveis armazenados em ambientes cloud.

Preparar e planear parece ser o caminho, a julgar pelo [estudo da Gartner](#) (2023). O mesmo revelou que 81% das organizações adotam uma estratégia multicloud e utilizam múltiplos fornecedores na nuvem, o que aumenta a complexidade da segurança e reforça a necessidade de uma abordagem integrada para proteger os dados e a infraestrutura. Além disso, uma [investigação da IBM](#) (2023) mostrou que muitas organizações ainda subestimam os desafios e custos associados à migração para cloud, o que inclui problemas com a conectividade da rede ou a complexidade no processo. A empresa alerta para a necessidade de uma maior consciencialização e um melhor planeamento estratégico para proteger os dados neste ambiente em rápida expansão.

PRINCIPAIS DESAFIOS

Configurações incorretas na nuvem são uma das principais causas de violação dos dados.

As organizações ficam vulneráveis a falhas de segurança de terceiros, como fornecedores.

Diferentes jurisdições impõem regras específicas para armazenamento e transferência de dados.



O QUE ESPERAR DE 2025?

Tecnologias como a computação confidencial e a segurança baseada em hardware (chips de segurança ou dispositivos especializados) vão transformar a proteção de dados na nuvem. Além disso, são de esperar padrões internacionais mais claros para operações multicloud, de forma a garantir um maior alinhamento entre diferentes regiões.

08

Transferência de dados e padrões de privacidade

A transferência internacional de dados faz parte do dia a dia das organizações com alcance global, mas também representa um desafio significativo, no que diz respeito à privacidade e conformidade regulatória.



Transferência de dados e padrões de privacidade



O RGPD introduziu normas rigorosas para as transferências transfronteiriças e destacou a importância de proteger informações pessoais num mundo digitalizado e globalizado. Decisões judiciais, como o caso Schrems II, redobram o escrutínio sobre as práticas de transferência de dados adotadas pelas organizações. A decisão invalidou o Privacy Shield e destacou as falhas na proteção de dados pessoais entre a União Europeia e os EUA, especialmente devido às leis de vigilância em massa. A decisão obrigou muitas empresas a reverem os seus processos e a adotarem novas soluções de conformidade, como as Standard Contractual Clauses (SCC). Além disso, trouxe à tona a necessidade de uma maior adaptação dos sistemas de gestão para proteção de dados e mitigação de riscos a diferentes realidades, regulações e idiomas – para garantir, em simultâneo, a conformidade com as exigências e legislações locais e internacionais.

No seguimento, em 2023, foi estabelecida a Data Privacy Framework entre os EUA e a União Europeia, como tentativa de superar os desafios de conformidade intercontinentais. No mesmo ano, o Japão firmou um acordo com os EUA (Japan-U.S. Data Privacy Framework), que permite a transferência

de dados entre os dois países e zela para que as empresas norte-americanas que lidam com dados de cidadãos japoneses cumpram exigências rigorosas de proteção e privacidade.

Após a decisão Schrems II, empresas como a Microsoft ajustaram as suas estratégias e criaram regiões de dados dedicadas na Europa para responderem aos requisitos regulatórios. Também o TikTok enfrentou uma pressão global para armazenar os dados localmente, tendo implementado medidas que garantem que as informações dos utilizadores são mantidas em regiões específicas, como os EUA e a Europa, em resposta às crescentes preocupações de privacidade.

Trata-se de um tema relevante, mas complexo. Um [relatório do EDPB](#), o European Data Protection Board, (2024) revelou que 55% das empresas enfrentam dificuldades na implementação de soluções técnicas para garantir a conformidade nas transferências internacionais de dados. E a [Ipsos](#) (2023) mostrou que uma fatia significativa dos consumidores demonstra preocupação com o envio dos seus dados para outros países, o que destaca a necessidade de uma maior transparência e confiança no tratamento de tais informações.

PRINCIPAIS DESAFIOS

As diferenças entre regulações dificultam as transferências seguras.

Garantir a conformidade exige, às empresas globais, investimentos significativos em recursos e tecnologias.

As transferências de dados críticos requerem maior proteção e escrutínio.



O QUE ESPERAR DE 2025?

Ferramentas de pseudonimização (substituição de indicadores pessoais) e criptografia avançada vão desempenhar um papel relevante na proteção de dados durante as transferências. Além disso, espera-se um avanço nas negociações para a criação de padrões globais de privacidade que facilitem o comércio internacional.

09

Avanços na autenticação e verificação de identidade

O aumento dos ciberataques impulsionou a evolução dos sistemas de autenticação, com o objetivo de reforçar a segurança e proporcionar uma experiência de utilizador mais fluida.



Avanços na autenticação e verificação de identidade



Métodos tradicionais, como o uso de senhas, estão a ser gradualmente substituídos ou complementados por tecnologias mais avançadas – como biometria, autenticação multifator (MFA) e soluções sem senha (passwordless). Estas inovações são desenhadas e implementadas para reduzir vulnerabilidades e acompanhar as crescentes exigências por maior proteção de dados.

Empresas como a Google e a Apple lideram a adoção da autenticação sem senha, com a utilização de chaves de segurança e biometria integrada (reconhecimento facial e leitura de impressões digitais), o que proporciona uma maior conveniência e proteção. A União Europeia, por outro lado, lançou o [European Digital Identity Wallet](#), uma iniciativa que promove uma identificação digital unificada, segura e acessível, e permite aos cidadãos controlarem as suas informações pessoais para o acesso a uma ampla gama de serviços públicos e privados em todo o espaço europeu.

Estudos recentes reforçam a importância destas mudanças na autenticação. Um [estudo da SailPoint](#) (2024) revela que a autenticação sem senha está a tornar-se uma tendência entre as organizações, com muitas a planearem adotar esta tecnologia até 2026, de forma a melhorarem a segurança e a eficiência no processo de

autenticação. Também uma [investigação da Mastercard](#) (2022) revelou que 74% dos consumidores latino-americanos preferem métodos biométricos devido à conveniência e à perceção de maior segurança, devido à conveniência.

À medida que as tecnologias de autenticação evoluem, surge a necessidade de novas abordagens para a gestão de identidades digitais. A autenticação adaptativa, que ajusta a verificação com base no risco de acesso, permite uma maior segurança sem prejudicar a experiência do utilizador. A integração de IA e machine learning permite detetar comportamentos anómalos em tempo real e bloqueia tentativas de acesso não autorizado antes que estas aconteçam.

Estas inovações exigem uma colaboração estreita e contínua entre governos, empresas e especialistas em segurança, sendo a meta não apenas impulsionar a inovação tecnológica, mas também garantir que a privacidade e a proteção de dados sejam integradas de forma proativa em todas as fases do desenvolvimento. Ao equilibrar os avanços tecnológicos com uma regulação eficaz, torna-se possível criar um ambiente digital mais seguro e confiável para os utilizadores, bem como promover um futuro no qual a segurança é um pilar essencial da transformação digital.

PRINCIPAIS DESAFIOS

Os sistemas biométricos levantam preocupações sobre vigilância e uso indevido de dados.

As tecnologias avançadas nem sempre estão disponíveis para todas as populações.

As organizações enfrentam desafios de investimento para adotar as soluções mais seguras e avançadas.



O QUE ESPERAR DE 2025?

A autenticação vai ser cada vez mais integrada a dispositivos pessoais e wearables (como smartphones, smartwatches, pulseiras de fitness ou dispositivos de segurança corporativa), enquanto tecnologias como blockchain poderão ser usadas para garantir identidades descentralizadas e seguras.

10

Pressão do cidadão/ consumidor por mais transparência e proteção

Os cidadãos e os consumidores estão cada vez mais conscientes dos riscos associados à recolha e à utilização de dados pessoais – exigem, por isso, maior transparência e responsabilidade por parte das empresas e organizações.



Pressão do cidadão/consumidor por mais transparência e proteção



Movimentos sociais, comunicação social e entidades movidas pela defesa da privacidade têm exercido pressão sobre empresas e governos para adotarem práticas mais éticas e seguras no tratamento de informações pessoais.

No setor público, e graças ao aumento das interações digitais com os serviços públicos, os cidadãos exigem maior controlo sobre os seus dados pessoais. Iniciativas legislativas como o [Digital Services Act](#) (DAS) na União Europeia refletem esta crescente exigência por proteção mais reforçada contra abusos em plataformas digitais. Os cidadãos esperam que os governos implementem padrões claros de segurança e privacidade para a proteção de dados sensíveis em interações digitais.

Já no setor empresarial, plataformas como a Signal e a DuckDuckGo ganharam relevância ao darem prioridade à privacidade dos utilizadores, demonstrando que é possível oferecer serviços digitais eficazes sem comprometer dados sensíveis. Mais organizações estão a reagir a esta procura, com empresas como a Apple a implementarem recursos inovadores (App Tracking Transparency), que permitem aos utilizadores bloquearem o rastreamento

das suas informações, reforçando assim o compromisso com a privacidade.

Investigações recentes confirmam a relevância desta mudança. Um [estudo da Pew Research](#) (2023) revelou que 79% dos utilizadores desejam mais controlo sobre como os seus dados são utilizados. Já um [relatório da Forrester](#) (2024) indicou que as marcas que adotam práticas transparentes têm mais probabilidade de fidelizar os seus consumidores. Estes dados mostram que a transparência e a proteção da privacidade não são apenas responsabilidade ética, mas também diferenciadores estratégicos no mercado atual.

PRINCIPAIS DESAFIOS

Independentemente das implicações tecnológicas, os consumidores e cidadãos esperam proteção.

A transparência sobre o uso de dados é cada vez mais exigida também pelos stakeholders.

Provar o compromisso com a privacidade em contexto de IA é um novo requisito para a confiança pública.



O QUE ESPERAR DE 2025?

Empresas que dão prioridade à ética e à transparência vão ser recompensadas com maior lealdade por parte dos consumidores. Da mesma forma, os governos que adotarem abordagens claras e inovadoras na proteção de dados terão mais confiança e adesão por parte dos cidadãos. Ferramentas como painéis de controlo de dados pessoais, que permitam aos utilizadores e cidadãos gerirem as suas informações diretamente, vão ganhar popularidade e criar um novo paradigma de transparência e segurança nos setores empresarial e público.



| Conclusão

E no final, tal como no princípio, as pessoas

Esta podia ser a previsão número 11 deste e-book, sobre os novos perfis profissionais dedicados à proteção de dados. Porquê? Porque na era digital, é fácil cair na tentação de nos focarmos apenas na tecnologia, como se ela fosse a única força transformadora. Mas, se há uma lição que aprendemos ao longo de décadas de inovação, é que a verdadeira transformação só ocorre quando as pessoas estão no seu centro.

Não se trata apenas de desenvolver sistemas de gestão, monitorização ou auditoria robustos que cumpram e façam cumprir regulações avançadas. Trata-se de nutrir uma cultura organizacional que reconheça que cada indivíduo – de um legislador a um software developer ou a um auditor – tem um papel fundamental no processo.

A responsabilidade pela proteção de dados e pela criação de um ecossistema digital ético não recai apenas sobre os DPO (Data Protection Officer) e CISO (Chief Information Security Officer), entendidos comumente como os grandes guardiões da conformidade nas organizações. Esta é uma missão coletiva.

As organizações que compreenderem a importância de formar profissionais especialistas em proteção de dados em todas as áreas, seja no marketing, na consultoria de negócios ou nas TI, e capacitarem as suas equipas para proteger a confiança do cidadão e do consumidor, terão uma posição de liderança no mercado e uma base sólida de confiança e inovação que lhes permitirá prosperar num ambiente digital em constante evolução.

Investir em tecnologia sem investir nas pessoas que a utilizam, que a validam, que a descomplicam através de formação ou sensibilização e que a desafiam, é um erro crasso. São as pessoas que, com a sua ética, competência e visão, vão garantir que a inovação não só acontece, mas acontece da maneira certa – de forma segura, transparente e responsável.

O equilíbrio entre a tecnologia, a regulação e o fator humano não é apenas uma estratégia inteligente. É, sem dúvida, a única forma de garantir que a evolução digital aplicada à proteção de dados nos beneficia a todos.

Agora que já conhece as 10 (quase 11) previsões para 2025, descubra a solução da Quidgest que ajuda a sua organização a enfrentar os desafios mais relevantes na área da privacidade de dados:

Solução de Gestão de Proteção de Dados Quidgest

Sabia que esta foi a primeira solução de gestão integrada no mercado que respondeu aos requisitos do RGPD? Esta ferramenta ajuda as organizações a cumprirem as regulações do setor e salvaguarda a segurança e a privacidade no tratamento de dados pessoais.

Esta solução garante:

- Estabilidade e consistência operacional
- Automação de tarefas complexas
- Redução de erros e riscos
- Agilização dos processos de comunicação com a CNPD
- Otimização de custos

SAIBA MAIS



As soluções da Quidgest destacam-se pela flexibilidade e adaptação a cada organização. Com a tecnologia Genio, são rapidamente ajustadas às necessidades específicas de cada cliente e às constantes evoluções tecnológicas e regulatórias.

A par da Gestão de Proteção de Dados, a Quidgest disponibiliza um conjunto de soluções avançadas que ajudam a garantir a conformidade da sua organização:

- **GESTÃO INTELIGENTE DE AUDITORIAS**

Planeie, execute e acompanhe auditorias com eficiência, garantindo total transparência nos processos.

- **GESTÃO DE RISCO E COMPLIANCE**

Antecipe riscos e assegure a conformidade com uma plataforma integrada.

- **AI ACT COMPLIANCE HUB**

Garanta a conformidade com o regulamento europeu de IA, protegendo a inovação e a ética

- **PORTAL CONFIDENCIAL DE DENÚNCIAS**

Facilite a comunicação segura e anónima de irregularidades, promovendo a confiança organizacional.

- **GESTÃO DE REPORTES REGULATÓRIOS**

Automatize e simplifique os reportes obrigatórios para uma resposta rápida aos reguladores.

- **MONITORIZAÇÃO DE SUSTENTABILIDADE EMPRESARIAL (ESG)**

Acompanhe e melhore o impacto ambiental e social da sua organização, em linha com práticas responsáveis.

Contacte-nos para saber mais:

solutions@quidgest.com

QUIDGEST

R. Viriato 7, 1050-233 Lisboa - Portugal

(+351) 213 870 563

quidgest@quidgest.com

www.quidgest.com

