PRIVUS MONTH INSIGHTS · Nº 3 · SETEMBRO 2026

RGPD · CONTINUIDADE DE NEGÓCIO · ISO 22301

Continuidade de negócio: a obrigação que o RGPD pressupõe e a ISO 22301 formaliza

Disponibilidade, resiliência e recuperação não são apenas controlos técnicos. Quando integradas com continuidade de negócio, tornam-se capacidade operacional demonstrável.

A obrigação implícita

O Regulamento Geral de Proteção de Dados exige disponibilidade, resiliência e capacidade de recuperação atempada. Não utiliza, contudo, expressamente o termo "continuidade de negócio".

Apesar de esta exigência estar subentendida, a lacuna terminológica tem um custo real: leva muitas organizações a tratar o artigo 32.º como um conjunto de requisitos técnicos dispersos, frequentemente reduzidos a backups e redundância pontual, em vez de o reconhecerem como aquilo que efetivamente pressupõe: uma obrigação sistémica, integrada no modelo operacional da organização.

A base jurídica é suficientemente clara. As Orientações n.º 9/2022 do Comité Europeu para a Proteção de Dados confirmam que uma perda temporária de disponibilidade de dados pessoais pode, por si só, constituir uma violação de dados pessoais, mesmo sem qualquer comprometimento da confidencialidade ou da integridade. A disponibilidade dos dados constitui, portanto, um requisito autónomo de conformidade.

O próprio Comité utiliza exemplos como uma falha de energia ou um ataque de negação de serviço que torne dados pessoais indisponíveis. Estes eventos podem configurar uma violação de dados pessoais, ficando a obrigação de notificação prevista no artigo 33.º dependente da subsequente avaliação do risco para os direitos e liberdades das pessoas singulares.

Outra confusão comum neste espaço consiste em assumir que maturidade em segurança da informação resolve, por inteiro, o problema da continuidade. Não resolve, pelo menos não sozinha.

A ISO/IEC 27001:2022 já contempla controlos relacionados com continuidade no seu Anexo A. Contudo, estes integram um conjunto mais amplo de medidas de segurança cuja aplicabilidade deve ser determinada e justificada através da avaliação de risco e refletida na Declaração de Aplicabilidade (SoA). A ISO 22301 inverte esta lógica: a continuidade deixa de ser um controlo entre muitos outros e passa a constituir o próprio objeto do sistema de gestão, com requisitos específicos de análise de impacto, definição de estratégias, preparação, resposta, testes, exercícios e melhoria contínua.

Uma organização pode, por isso, apresentar um elevado nível de conformidade em segurança da informação e continuar operacionalmente incapaz de restaurar serviços críticos dentro dos tempos necessários quando ocorre um incidente. A profundidade de exigência entre os dois instrumentos não é a mesma.

Da teoria à prática

A teoria é clara. A prática, como os exemplos seguintes demonstram, tende a ficar aquém dela.

Os últimos anos oferecem exemplos claros deste gap, em geografias distintas e sem relação direta entre si.

Em fevereiro de 2022, uma operadora de telecomunicações portuguesa sofreu uma interrupção que afetou rede móvel, SMS e canais de apoio ao cliente durante vários dias, produzindo efeitos em cascata sobre serviços de emergência, pagamentos e outras organizações dependentes daquela infraestrutura sem redundância própria.

Em julho de 2026, uma operadora angolana com mais de 20 milhões de clientes sofreu uma interrupção nacional da rede na proximidade da sua estreia em bolsa. O episódio constituiu mais um lembrete de que uma falha operacional numa infraestrutura com elevada concentração de mercado pode rapidamente ultrapassar a dimensão tecnológica e transformar-se num problema de continuidade, reputação e dependência sistémica para clientes, parceiros e serviços dependentes.

No Reino Unido, o TSB Bank foi multado em £48,65 milhões em 2022 na sequência de falhas graves de governação e gestão do risco operacional associadas a uma migração de sistemas que deixou milhões de clientes sem acesso adequado às suas contas e serviços bancários. O próprio regulador descreveu o sucesso da migração como determinante para a capacidade do banco de assegurar a continuidade das suas funções críticas. É a mesma exigência que, no RGPD, aparece sob a forma de disponibilidade e resiliência.

No Brasil, a Lojas Renner, vítima de ransomware em 2021, conseguiu restabelecer uma parte substancial das suas operações comerciais num período relativamente curto, após cerca de 48 horas de indisponibilidade dos canais digitais. O caso demonstra a importância prática da capacidade de recuperação quando um incidente começa a afetar diretamente a operação.

A exposição em números

Os números reforçam a dimensão do problema.

Em Portugal, o CERT.PT registou 2.758 incidentes de cibersegurança em 2024, um aumento de aproximadamente 36% face ao ano anterior. Cerca de 78% dos incidentes registados ocorreram em entidades privadas.

Em África, os dados relativos a 2025 mostram uma exposição particularmente elevada. O African Cyberthreat Assessment Report 2026, da INTERPOL, coloca Angola em primeiro lugar nas deteções de botnets em África naquele ano, representando 37,95% das deteções consideradas no relatório.

Globalmente, segundo o Cost of a Data Breach Report 2025, da IBM e do Ponemon Institute, 65% das organizações analisadas ainda não tinham recuperado completamente da violação de dados sofrida. Mesmo entre aquelas que declararam recuperação completa, 76% demoraram mais de 100 dias a alcançá-la. É precisamente o oposto da lógica de restauração atempada que o RGPD procura assegurar.

O risco real

O risco real não é apenas sofrer o incidente. É descobrir, durante o incidente, que a organização nunca definiu quanto tempo pode ficar parada.

Do RGPD à NIS2

Este movimento também não se esgota no RGPD. Para as entidades essenciais e importantes abrangidas pela NIS2, designadamente em setores como telecomunicações, energia e infraestrutura digital, a continuidade de negócio surge já formalizada como categoria autónoma de medidas de gestão do risco de cibersegurança. A orientação regulatória europeia aponta cada vez mais para planos documentados, responsabilidades claras, capacidade de recuperação, testes, exercícios e articulação entre continuidade, backup, gestão de crises e resposta a incidentes.

Aquilo que no RGPD surge, em grande medida, através das exigências de disponibilidade, resiliência e recuperação, transforma-se, para um número crescente de setores, num requisito explícito de governação e de auditoria. A direção do movimento regulatório é inequívoca, ainda que o seu alcance não seja universal.

O problema da fragmentação

O que estes casos e estes números têm em comum é a fragmentação dos frameworks de compliance dentro das organizações. RGPD, ISO 27001 e ISO 22301 são frequentemente tratados como exercícios paralelos: cada um responde à sua auditoria, ao seu responsável e à sua documentação, sem um sistema comum que os ligue. É também aqui que a maioria das abordagens de consultoria tradicional falha: tratam cada referencial como um projeto isolado, com equipas, prazos e entregáveis próprios, em vez de o desenharem como um sistema único desde o início.

É precisamente aí que surge a exposição. Uma organização pode ter política de segurança, backups, plano de resposta a incidentes e dezenas de evidências documentais e, ainda assim, não saber responder a três perguntas elementares quando um serviço crítico deixa de funcionar.

A vantagem de integrar os três referenciais vai, por isso, além de evitar coimas ou reduzir o desgaste reputacional associado a um incidente mal gerido: é também operacional e competitiva. Significa recuperar mais depressa, reduzir impacto financeiro, demonstrar maturidade perante clientes, parceiros, seguradoras e investidores e transformar aquilo que muitas organizações continuam a tratar exclusivamente como custo de conformidade num diferencial verificável de confiança e, consequentemente, numa vantagem competitiva.

Para qualquer Conselho de Administração

As perguntas que ficam para qualquer Conselho de Administração são simples:

01 **A organização já realizou uma BIA (Business Impact Analysis)?**

02 **Qual é o seu RPO (Recovery Point Objective)?**

03 **Qual é o seu RTO (Recovery Time Objective)?**

04 **E, mais do que isso: a sua empresa tem um mapa de interseção dos vários frameworks de compliance a que está sujeita?**

Se estas respostas não existem, não estão aprovadas ou nunca foram testadas, a organização pode estar documentalmente conforme e, ainda assim, operacionalmente exposta.

"A evidência é a alma do compliance."

A Privus Kuzola audita a integração entre RGPD, ISO 27001 e ISO 22301, identificando onde a sua organização está documentalmente conforme, mas operacionalmente exposta.

Conheça a intervenção da Privus em ISO 22301.

Fontes

1. Comité Europeu para a Proteção de Dados (EDPB), *Guidelines 9/2022 on personal data breach notification under GDPR*, versão 2.0.

2. Regulamento (UE) 2016/679, RGPD, designadamente artigo 32.º.

3. Diretiva (UE) 2022/2555, NIS2, designadamente artigo 21.º.

4. ENISA, *Threat Landscape 2025*.

5. ENISA, *NIS2 Technical Implementation Guidance*.

6. Centro Nacional de Cibersegurança (CNCS), *Relatório Cibersegurança em Portugal - Riscos & Conflitos*, 6.ª edição, 2025.

7. INTERPOL, *African Cyberthreat Assessment Report 2026*.

8. IBM / Ponemon Institute, *Cost of a Data Breach Report 2025*.

9. Financial Conduct Authority (FCA) e Prudential Regulation Authority (PRA), comunicado sobre a coima ao TSB Bank plc, dezembro de 2022.

10. PÚBLICO, "Ataque à Vodafone. O que foi afectado e o que já está resolvido?", 8 de fevereiro de 2022.

11. Vodafone Portugal, comunicado sobre o ciberataque de fevereiro de 2022.

12. Observador, "Ataque informático deixa milhões de clientes da angolana Unitel sem rede na véspera da estreia em bolsa", 28 de julho de 2026.

13. Exame, cobertura da recuperação da Lojas Renner após o ataque informático, agosto de 2021.

Conteúdo informativo e geral. Não constitui parecer jurídico, auditoria, certificação ou recomendação aplicável sem análise do contexto concreto.

Para conversar sobre o contexto da sua organização: contacto@privuskuzola.pt · +351 936 246 971