

Política de Continuidade de Negócio, Backup e Recuperação de Desastres

Compromissos e princípios de preparação, resposta e recuperação de serviços perante interrupções relevantes.

REFERÊNCIA	VERSÃO	DATA	CLASSIFICAÇÃO
NW-BCP-001	3.0	10/10/2026	PÚBLICO

NEXTWEB – PRESTAÇÃO DE SERVIÇOS NA ÁREA DA INTERNET LDA.

Rua António Lima Fragoso, 145 · 3060-216 Cantanhede · www.nextweb.pt

1. Objetivo e âmbito

A Nextweb reconhece que a disponibilidade dos serviços tecnológicos e a integridade da informação são essenciais à atividade dos seus clientes. Esta política estabelece princípios institucionais para identificar funções críticas, reduzir a probabilidade e impacto de interrupções e orientar a recuperação proporcional ao risco e às condições efetivamente contratadas.

A política abrange infraestruturas e serviços sob gestão da Nextweb, processos internos essenciais, relações com fornecedores críticos e canais de comunicação necessários em contingência. Os planos técnicos, localizações, contactos individuais, inventários de ativos e esquemas de redundância são reservados.

2. Continuidade de negócio e recuperação tecnológica

Continuidade de negócio consiste na capacidade organizacional de preservar ou retomar funções prioritárias perante uma interrupção. Recuperação de desastres diz respeito aos meios e procedimentos para restaurar sistemas, redes, aplicações, dados e dependências técnicas afetadas.

A estratégia articula três dimensões: administração e comunicação da crise (PAC), continuidade operacional (PCO) e recuperação tecnológica (PRD), preservando o enquadramento já adotado nos planos históricos da Nextweb.

3. Identificação de processos e análise de impacto

Os processos críticos são identificados segundo relevância operacional, compromissos com clientes, impacto financeiro, segurança, disponibilidade de pessoal e dependências técnicas. A análise de impacto no negócio (BIA) permite estabelecer prioridades e avaliar os efeitos da interrupção ao longo do tempo.

MTD representa a interrupção máxima tolerável de uma função; RTO representa o objetivo de tempo de reposição; RPO representa a perda de dados aceitável medida no tempo; WRT representa o trabalho necessário para reconstituir e validar o funcionamento do processo depois do restabelecimento técnico. Estes parâmetros variam por serviço e são definidos em instrumentos operacionais ou contratuais, não devendo ser presumidos uniformes.

4. Cenários de risco considerados

Podem justificar ações de contingência incidentes de energia elétrica, incêndio, inundação, indisponibilidade das instalações, falhas de conectividade, hardware ou sistemas operativos, comprometimento de identidades, ataques informáticos, corrupção ou perda de dados, indisponibilidade de fornecedores e erro humano.

A avaliação pondera impacto na informação, disponibilidade de serviços, segurança de pessoas, obrigações contratuais e legais, capacidade de recuperação e riscos de propagação do incidente.

5. Estratégia de backup e preservação de dados

Os procedimentos de salvaguarda são definidos em função da criticidade dos dados, responsabilidades contratuais, capacidade técnica e recursos disponíveis. Podem incluir cópias locais e remotas, cópias protegidas contra alteração, controlos de acesso, encriptação, monitorização e procedimentos de recuperação testáveis.

Frequências, retenções, janelas, tipo de cópia, exclusões e responsabilidades variam por serviço ou cliente e devem constar do contrato, catálogo de serviço ou especificação técnica aplicável. A contratação de um serviço de alojamento ou suporte não pressupõe, por si só, a inclusão de backups geridos.

6. Redundância, energia e dependências externas

São avaliadas medidas proporcionais de redundância, alimentação de emergência, proteção elétrica, comunicações alternativas, capacidade de substituição de equipamentos e recuperação em ambiente secundário quando disponíveis e pertinentes.

Os mecanismos dependem de infraestrutura física, autonomia real dos sistemas, fornecedores e condições contratuais. Não são afirmados neste documento valores absolutos de autonomia, replicação em tempo real ou disponibilidade universal.

7. Detecção, escalamento e declaração de contingência

As anomalias que coloquem em risco um processo relevante são comunicadas para análise da equipa responsável. A decisão de ativar medidas de contingência considera âmbito, gravidade, duração previsível e capacidade de resolução, com articulação com a Gerência quando necessário.

Podem ser adotadas medidas graduais, desde intervenção técnica localizada até à mobilização de recursos alternativos e formalização de situação de crise. Os procedimentos internos identificam responsabilidades, substituições, contactos e decisões autorizadas.

8. Recuperação e regresso à normalidade

A recuperação é conduzida de acordo com a segurança das pessoas e a prioridade dos serviços, incluindo avaliação das causas, isolamento de riscos, reposição de conectividade, restauro de sistemas e dados, testes funcionais e validação antes da retoma definitiva.

O encerramento do incidente é acompanhado, conforme aplicável, por comunicação aos interessados, revisão de evidências e identificação de melhorias. A retoma deve evitar a reintrodução de ameaças ainda ativas.

9. Comunicação com clientes e autoridades

Quando uma interrupção tiver impacto relevante em clientes, as comunicações procuram informar com rigor a natureza do evento, serviços afetados, medidas de mitigação e evolução conhecida, sem divulgar elementos confidenciais ou comprometer investigações.

São observados os deveres de notificação decorrentes de proteção de dados, cibersegurança, telecomunicações e outros regimes aplicáveis, segundo o enquadramento da atividade e as

obrigações contratuais.

10. Testes, sensibilização e melhoria

Os procedimentos de continuidade devem ser revistos e exercitados periodicamente mediante cenários proporcionais ao risco, procurando não prejudicar a operação produtiva. A aprendizagem recolhida em testes e incidentes suporta a atualização dos planos, formação dos envolvidos e prevenção de reincidências.

11. Limitações e condições de serviço

Os compromissos de continuidade, níveis de serviço, prazos de recuperação e exclusões são os expressamente acordados para cada serviço. Esta política apresenta a abordagem geral de gestão da continuidade e não constitui garantia autónoma de disponibilidade ininterrupta, cópia integral de todos os dados ou reposição em prazo fixo.

Em particular, serviços operados em infraestrutura do cliente podem depender de licenças, autorizações de acesso, estado dos equipamentos, disponibilidade de cópias válidas e da colaboração do próprio cliente.