					Insira aqui a designação da entidade jurídica registada							
Número do documento: P32S					Título do documento: **Política de Continuidade do Negócio e Recuperação de Desastres**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 6.1, 6.3, 8	
ISO/IEC 27002:2022	Controlos 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
RGPD da UE	Artigos 32, 33	
Diretiva NIS2 da UE	Artigo 21(2)(f)	
DORA da UE	Artigo 10	
COBIT 2019	DSS04	

1. Finalidade

1.1 Esta política assegura que a organização consegue manter as operações de negócio e recuperar serviços de TI essenciais durante e após eventos disruptivos, tais como falhas de energia, ciberataques, infeções por ransomware ou falhas de sistema.

1.2 Esta política estabelece um quadro claro para o planeamento da continuidade do negócio e da recuperação de desastres (BC/DR), adequado a PME sem equipas de TI dedicadas.

1.3 Esta política ajuda a organização a cumprir requisitos obrigatórios ao abrigo da ISO/IEC 27001:2022, do RGPD da UE, da Diretiva NIS2 da UE, da DORA da UE e do COBIT 2019, reforçando simultaneamente a resiliência operacional e a confiança dos clientes.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os sistemas e serviços críticos para o negócio (por exemplo, correio eletrónico, armazenamento na nuvem, plataformas de faturação, registos de clientes)

2.1.2 Todos os trabalhadores e prestadores externos de serviços de TI responsáveis pela preparação e execução de BC/DR

2.1.3 Todos os tipos de disrupção, incluindo incidentes cibernéticos, falhas de hardware, falhas de energia, inundações e inacessibilidade ao escritório

2.2 Esta política abrange:

2.2.1 a gestão de cópias de segurança

2.2.2 o planeamento da continuidade do negócio (BCP)

2.2.3 as operações de recuperação de desastres

2.2.4 a formação e os testes do pessoal

2.2.5 os procedimentos de resposta legal e regulamentar

3. Objetivos

3.1 Proteger a capacidade da organização para prestar serviços essenciais apesar de disrupções não planeadas.

3.2 Assegurar a recuperação atempada de sistemas e dados com Objetivos de Tempo de Recuperação (RTO) previamente definidos.

3.3 Permitir que todo o pessoal siga os procedimentos de continuidade durante situações de crise com o mínimo de confusão.

3.4 Manter o cumprimento dos requisitos regulamentares em matéria de proteção de dados e resiliência operacional, incluindo o artigo 32.º do RGPD da UE e o artigo 21.º da Diretiva NIS2 da UE.

3.5 Estabelecer uma estratégia prática e testável de continuidade e recuperação adequada a PME.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 É o responsável pelo processo de BC/DR e pela presente política

4.1.2 Aprova o Plano de Continuidade do Negócio (BCP)

4.1.3 Coordena a resposta a incidentes e a comunicação interna durante disrupções

4.1.4 Efetua notificações regulamentares, quando aplicável (por exemplo, notificações de violação de dados ao abrigo do RGPD da UE)

4.2 Prestador de suporte de TI / administrador de sistemas

4.2.1 Mantém e testa as cópias de segurança

4.2.2 Executa os procedimentos de recuperação de desastres quando acionados

4.2.3 Documenta todas as ações de recuperação e eventos de restauro de sistemas

4.2.4 Reporta imediatamente ao GM os incidentes críticos de TI

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1 Revisão anual da política e do plano

9.1.1 O Diretor-Geral (GM) deve assegurar que esta política e o respetivo Plano de Continuidade do Negócio (BCP) são formalmente revistos pelo menos uma vez por ano.

9.1.2 A revisão deve incluir:

9.1.2.1 avaliação de riscos novos ou emergentes

9.1.2.2 revalidação de RTO/RPO

9.1.2.3 verificação da informação de fornecedores e contactos

9.1.2.4 alinhamento com alterações em sistemas de TI, obrigações legais ou operações

9.2 Atualizações acionadas por eventos

9.2.1 Esta política deve também ser atualizada em resposta a:

9.2.1.1 incidentes ou disrupções relevantes, especialmente se os objetivos não tiverem sido atingidos

9.2.1.2 novas obrigações legais ou regulamentares (por exemplo, alterações à DORA da UE)

9.2.1.3 alterações em sistemas críticos, plataformas cloud ou pessoal

9.2.1.4 conclusões dos testes anuais de BCP/DR

9.3 Processo de controlo de alterações

9.3.1 Todas as alterações devem ser aprovadas pelo GM

9.3.2 Deve ser mantido um registo histórico de versões, incluindo data, descrição da alteração e aprovador

9.3.3 A política atualizada deve ser redistribuída a todo o pessoal relevante, incluindo o prestador de suporte de TI e os responsáveis de departamento

9.4 Documentação de lições aprendidas

9.4.1 Após testes ou disrupções reais, as lições aprendidas documentadas devem ser incorporadas em revisões futuras

9.4.2 Estas revisões devem igualmente incluir avaliações do desempenho dos fornecedores e verificações da adequação da resposta

10. Políticas relacionadas e interligações

10.1 Esta política está estreitamente integrada com as seguintes políticas SME:

10.1.1 P1S – Política de Segurança da Informação: define os objetivos de segurança de alto nível que as práticas de continuidade e recuperação devem suportar.

10.1.2 P4S – Política de Controlo de Acesso: permite a revogação de acessos de emergência ou o restabelecimento de acessos de utilizadores em cenários de disrupção do negócio.

10.1.3 P6S – Política de Gestão de Riscos: constitui a base para identificar, avaliar e priorizar riscos relacionados com a continuidade.

10.1.4 P8S – Política de Sensibilização e Formação em Segurança da Informação: assegura que os trabalhadores estão preparados para agir durante disrupções e compreendem o BCP.

10.1.5 P15S – Política de Cópias de Segurança e Restauro: estabelece procedimentos técnicos específicos para salvaguardar a disponibilidade dos dados e a recuperação.

10.1.6 P17S – Política de Proteção de Dados e Privacidade: assegura que o planeamento da continuidade respeita a proteção de dados pessoais e cumpre o RGPD da UE durante e após incidentes.

10.1.7 P22S – Política de Registo de Logs e Monitorização: suporta a deteção de eventos que podem acionar processos de BC/DR e fornece trilhos de auditoria forense após disrupções.

10.1.8 P30S – Política de Resposta a Incidentes: precede diretamente a ativação do processo de recuperação em caso de incidentes cibernéticos ou operacionais.

10.1.9 P31S – Política de Recolha de Evidência e Análise Forense: assegura que a evidência digital é recolhida em cenários de continuidade para fins de conformidade, seguros ou investigação.

10.2 Estas políticas formam um quadro coeso e preparado para auditoria em matéria de resiliência, responsabilização e continuidade dos controlos em todas as operações da PME.

11. Normas e referenciais de referência

11.1 ISO/IEC 27001:

11.1.1 A cláusula 6.1 exige planeamento e tratamento baseados no risco, incluindo continuidade do negócio e recuperação.

11.1.2 A cláusula 6.3 dá ênfase à melhoria contínua após disrupções.

11.1.3 A cláusula 8.1 impõe controlos operacionais, incluindo medidas de continuidade documentadas.

11.2 ISO/IEC 27002:

11.2.1 O controlo 5.29 exige o estabelecimento e a manutenção de mecanismos de continuidade do negócio.

11.2.2 O controlo 5.30 exige o teste e a revisão desses mecanismos.

11.3 NIST SP 800-53 Rev.5:

11.3.1 O CP-2 define requisitos para o planeamento de contingência.

11.3.2 O CP-4 impõe formação em contingência para o pessoal da organização.

11.3.3 O CP-6 abrange requisitos relativos a local alternativo de armazenamento.

11.3.4 O CP-7 regula expectativas relativas a local alternativo de processamento.

11.4 RGPD da UE:

11.4.1 O artigo 32.º exige medidas para assegurar a disponibilidade contínua e a resiliência dos sistemas e serviços de tratamento.

11.4.2 O artigo 33.º aciona obrigações de notificação de violação de dados nos casos em que uma falha de continuidade resulte em comprometimento de dados pessoais.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 O artigo 21(2)(f) exige capacidades de planeamento da continuidade e de gestão de crises como condição de preparação para riscos cibernéticos.

11.6 DORA da UE (2022/2554):

11.6.1 O artigo 10.º impõe a implementação de testes de resiliência operacional digital e capacidades de recuperação, especialmente para PME do setor financeiro.

11.7 COBIT 2019:

11.7.1 O DSS04 – Gerir a Continuidade fornece orientações de governação empresarial para manter e validar a resiliência operacional, incluindo responsabilidade, testes, integração de fornecedores e revisões pós-evento.