					Insira aqui a designação da entidade jurídica registada							
Número do documento: P32					Título do documento: **Política de Continuidade de 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	Cláusula 8	
ISO/IEC 27002:2022	Controlos 5.29, 5.30	
NIST SP 800-53 Rev. 5	CP-1 a CP-11	
NIST SP 800-34 Rev. 1	Planeamento de contingência	Referencial
ISO 22301:2019		Requisitos do Sistema de Gestão da Continuidade de Negócio
RGPD da UE	Artigo 32	
Diretiva NIS2 da UE	Artigo 21(2)(f)	
DORA da UE	Artigo 10	
COBIT 2019	DSS04	

1. Finalidade

1.1. Esta política define os controlos obrigatórios, bem como os papéis e responsabilidades, para assegurar a capacidade da organização de manter ou restabelecer operações críticas de negócio e os serviços de TIC de suporte durante e após um incidente disruptivo.

1.2. Esta política visa proteger a vida, a estabilidade operacional, as obrigações legais, os compromissos com clientes e a reputação da organização, incorporando resiliência através de planeamento proativo e de capacidades de recuperação validadas.

1.3. Esta política estabelece a base do quadro de continuidade de negócio e recuperação de desastres da organização, assegurando o cumprimento dos requisitos regulamentares, contratuais e setoriais aplicáveis.

2. Âmbito

2.1. Esta política aplica-se a todas as unidades organizacionais, sistemas de informação, processos de negócio, colaboradores e serviços de terceiros classificados como críticos ou essenciais com base nos resultados da análise de impacto no negócio.

2.2. A política abrange:

2.2.1. Disrupções naturais e provocadas pelo homem, incluindo ciberataques, falhas de infraestrutura, indisponibilidade de centros de dados, pandemias e interrupções de serviço de fornecedores

2.2.2. O planeamento, os testes e a melhoria contínua dos Planos de Continuidade de Negócio (BCP) e dos Planos de Recuperação de Desastres (DRP)

2.2.3. Papéis e responsabilidades para resposta a emergências, coordenação da recuperação e escalonamento de incidentes

2.3. Todos os colaboradores com responsabilidades de continuidade ou recuperação, incluindo TI, responsáveis de negócio, gestores de crise e fornecedores, estão sujeitos às disposições desta política.

3. Objetivos

3.1. Assegurar a continuidade das operações e dos serviços de negócio através de procedimentos predefinidos e testados, minimizando o impacto operacional, reputacional e legal.

3.2. Recuperar os serviços de TIC dentro dos objetivos de tempo de recuperação (RTO) e dos objetivos de ponto de recuperação (RPO) definidos, alinhados com os níveis de tolerância ao risco do negócio.

3.3. Atribuir a responsabilidade pelo planeamento, execução e governação da continuidade de negócio e da recuperação de desastres em toda a organização.

3.4. Assegurar que as capacidades de continuidade são testadas, mantidas e melhoradas regularmente com base em cenários realistas e em resultados de auditoria.

3.5. Cumprir as obrigações aplicáveis ao abrigo das normas ISO, NIST, RGPD, DORA e NIS2, suportando a devida diligência em matéria de resiliência operacional e disponibilidade.

4. Papéis e responsabilidades

4.1. Alta Direção

4.1.1. Aprova a Política de Continuidade de Negócio e Recuperação de Desastres e assegura o seu alinhamento estratégico.

4.1.2. Aloca orçamento e recursos para suportar a continuidade de negócio, a resposta a emergências e os exercícios de recuperação.

4.2. Gestor de Continuidade de Negócio (Líder de BCM)

4.2.1. É responsável pelo desenvolvimento e manutenção dos BCP em toda a organização e pela coordenação dos testes de continuidade.

4.2.2. Mantém o calendário da análise de impacto no negócio, promove a formação e assegura que a documentação cumpre os requisitos de conformidade.

[... 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. Esta política deve ser revista anualmente pelo Gestor de Continuidade de Negócio e pelo Diretor de Segurança da Informação, para assegurar o alinhamento com:

9.1.1. Alterações nas operações de negócio, nos sistemas críticos ou na infraestrutura

9.1.2. Lições aprendidas com incidentes, auditorias, exercícios de tabletop ou testes de recuperação de desastres

9.1.3. Obrigações regulamentares ou contratuais atualizadas (por exemplo, DORA, RGPD, requisitos de cliente relativos a RTO/RPO)

9.1.4. Alterações ao apetite ao risco da organização ou à estratégia de continuidade

9.2. As revisões devem incluir:

9.2.1. Validação da relevância dos planos e dos dados de contacto

9.2.2. Reavaliação de RTO, RPO e da estratificação de recuperação

9.2.3. Avaliação da capacidade do serviço de cópias de segurança e de recuperação de desastres

9.2.4. Feedback das partes interessadas que executaram planos ou testes de recuperação recentes

9.3. Todas as alterações às políticas devem:

9.3.1. Estar sujeitas a controlo de versões, com fundamentação documentada e aprovação formal das partes interessadas

9.3.2. Ser comunicadas aos colaboradores e às equipas relevantes com responsabilidades atualizadas

9.3.3. Refletir-se na formação, nos materiais de sensibilização e nos procedimentos operacionais atualizados

9.4. Devem ser emitidas atualizações intercalares de emergência sempre que exista uma alteração organizacional relevante, uma imposição legal ou uma constatação crítica que torne os planos ou a política em vigor inviáveis.

10. Políticas relacionadas e articulações

10.1. Esta política articula-se com os seguintes documentos principais:

10.1.1. P1 – Política de Segurança da Informação: estabelece o requisito de operações resilientes e baseadas no risco em todas as condições.

10.1.2. P5 – Política de Gestão de Alterações: assegura que quaisquer alterações de configuração ou de infraestrutura relacionadas com a recuperação seguem fluxos de trabalho documentados e aprovados.

10.1.3. P14 – Política de Retenção e Eliminação de Dados: rege o ciclo de vida dos suportes de cópia de segurança e dos dados recuperados utilizados nas operações de continuidade.

10.1.4. P15 – Política de Cópias de Segurança e Restauro: aplica controlos sobre a frequência, segurança e verificação do restauro de cópias de segurança.

10.1.5. P18 – Política de Controlos Criptográficos: assegura que os processos de recuperação mantêm as normas de cifragem e confidencialidade.

10.1.6. P22 – Política de Registo e Monitorização: suporta a deteção e o escalonamento de eventos com impacto na continuidade.

10.1.7. P30 – Política de Resposta a Incidentes: define os processos de contenção, escalonamento e análise de causa raiz alinhados com os acionadores de continuidade.

10.1.8. P33 – Política de Auditoria e Monitorização da Conformidade: valida a integridade e a eficácia das práticas de continuidade e recuperação em sistemas e processos.

11. Normas e referenciais

11.1. Esta política está alinhada com normas internacionalmente reconhecidas de continuidade de negócio e recuperação de desastres, suportando a auditabilidade, a resiliência e a conformidade legal.

11.2. ISO/IEC 27002

11.2.1. Controlo 5.29 do Anexo A – Segurança da informação durante disrupções: exige a continuidade dos controlos de segurança em condições adversas.

11.2.2. Controlo 5.30 do Anexo A – Prontidão das TIC para a continuidade de negócio: exige a preparação, o teste e a validação das capacidades de recuperação de TIC.

11.3. ISO 22301:2019 – Sistemas de Gestão da Continuidade de Negócio

11.3.1. Fornece o quadro de referência para estabelecer, implementar e manter práticas de continuidade de negócio alinhadas com os objetivos organizacionais e os limiares de risco.

11.4. NIST SP 800-34 Rev. 1 – Guia de planeamento de contingência

11.4.1. Estabelece as melhores práticas para planos de contingência de sistemas de TI, incluindo o desenvolvimento da estratégia de continuidade, a análise de impacto e os testes aos planos.

11.5. RGPD da UE (2016/679)

11.5.1. Artigo 32 – Segurança do tratamento: exige a resiliência dos sistemas de tratamento e o restauro atempado da disponibilidade e do acesso a dados pessoais após um incidente.

11.6. Diretiva NIS2 da UE (2022/2555)

11.6.1. Artigo 21(2)(f): impõe medidas de continuidade de negócio e de gestão de crises para suportar a segurança das redes e dos sistemas de informação.

11.7. DORA da UE (2022/2554)

11.7.1. Artigo 10 – Continuidade de negócio das TIC: exige que as entidades financeiras desenvolvam e testem planos de continuidade das TIC, incluindo RTO/RPO baseados no risco e capacidades de failover.

11.8. COBIT 2019

11.8.1. DSS04 – Gerir a continuidade: abrange todos os aspetos do planeamento da continuidade, incluindo a identificação de ameaças, análise de impacto, estratégia de recuperação e testes regulares.