					Insira aqui a designação da entidade jurídica registada							
Número do documento: P15S					Título do documento: **Política de Cópias de Segurança e Restauro**							
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**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	Controlos de cópias de segurança de acordo com os requisitos do SGSI
ISO/IEC 27002:2022	Controlos 5.29, 8	Melhores práticas para cópias de segurança e integração com o BCP
NIST SP 800-53 Rev.5	CP-9, MP-6	Cópias de segurança e proteção de suportes
Diretiva NIS2 da UE	Artigo 21(2)(c)	Resiliência e continuidade através de cópias de segurança
DORA da UE	Artigo 10(1)	Continuidade das TIC - cópias de segurança para organizações financeiras
COBIT 2019	BAI04.05, DSS04	Documentação e testes de cópias de segurança, processos de controlo
RGPD da UE	Artigos 5(1)(f), 32(1)(c)	Integridade, disponibilidade e restauro atempado dos dados

1. Finalidade

1.1 A presente política define a forma como a organização executa e gere as cópias de segurança, de modo a assegurar a continuidade do negócio, proteger contra a perda de dados e permitir a recuperação atempada após incidentes.

1.2 Estabelece regras vinculativas sobre a forma como os sistemas e os dados devem ser objeto de cópia de segurança, armazenamento e restauro, em particular em PME sem infraestruturas de TI complexas.

1.3 Esta política apoia a capacidade de demonstrar conformidade em auditoria e a certificação ISO/IEC 27001, assegurando que os controlos essenciais de cópias de segurança estão implementados, são aplicados de forma consistente e são revistos regularmente.

1.4 A capacidade da organização para recuperar de falhas técnicas, eliminação acidental ou incidentes de cibersegurança depende do cumprimento rigoroso desta política.

2. Âmbito

2.1 Esta política aplica-se a todos os sistemas empresariais e dados, incluindo:

2.1.1 Registos financeiros, informação de clientes e dados de recursos humanos

2.1.2 Computadores de secretária, computadores portáteis, servidores e aplicações na nuvem utilizados nas operações de negócio

2.1.3 Suportes de cópia de segurança, como unidades USB, armazenamento externo ou cópias de segurança alojadas na nuvem

2.2 Aplica-se igualmente a todas as pessoas com responsabilidade pelo tratamento ou gestão de processos de cópia de segurança, incluindo:

2.2.1 O Diretor-Geral (GM) ou a pessoa designada como responsável

2.2.2 Prestadores externos de serviços de TI ou consultores

2.2.3 Todos os trabalhadores responsáveis por guardar dados em localizações aprovadas

3. Objetivos

3.1 Assegurar que todos os dados e sistemas críticos para o negócio são objeto de cópia de segurança segura, em intervalos adequados, com base no risco e na necessidade operacional.

3.2 Garantir que os dados podem ser recuperados de forma atempada e integral após interrupções.

3.3 Prevenir o acesso não autorizado, a adulteração ou a perda de dados de cópia de segurança através de controlos de armazenamento eficazes.

3.4 Atribuir de forma clara e assegurar o cumprimento dos papéis e responsabilidades pela implementação e teste dos procedimentos de cópia de segurança.

3.5 Apoiar o cumprimento da ISO/IEC 27001, do RGPD da UE e de outras obrigações regulamentares através de práticas de cópia de segurança estruturadas e documentadas.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Aprova a presente política e assegura a sua aplicação

4.1.2 Aloca recursos e designa os responsáveis pelas atividades de cópia de segurança e restauro

4.1.3 Revê falhas de cópia de segurança, incidentes ou desvios à política

4.1.4 Realiza as revisões anuais da política e assegura a capacidade de demonstrar conformidade em auditoria

4.2 Prestador externo de suporte de TI (se aplicável)

4.2.1 Implementa e gere soluções de cópia de segurança (locais ou alojadas na nuvem)

4.2.2 Monitoriza o sucesso das cópias de segurança e agenda testes de restauro

4.2.3 Reporta falhas e incidentes diretamente ao GM

4.2.4 Assegura a cifragem, as restrições de acesso e o tratamento adequado dos suportes de cópia de segurança

[... 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 pelo menos uma vez por ano pelo GM. Os fatores desencadeadores de revisões intercalares incluem:

9.1.1 Alterações com impacto significativo em sistemas ou métodos de armazenamento

9.1.2 Introdução de novas plataformas na nuvem ou novas tecnologias de TI

9.1.3 Alterações legais ou regulamentares que afetem a recuperação de dados

9.1.4 Constatações de auditoria ou incidentes

9.2 O GM é responsável por iniciar a revisão, aprovar alterações e comunicar atualizações.

9.3 As versões da política devem ser controladas e arquivadas. As versões substituídas devem ter o acesso restringido para evitar confusão durante auditorias ou eventos de recuperação do negócio.

10. Políticas relacionadas e ligações

10.1 Esta política está alinhada com as seguintes políticas SME e delas depende:

10.1.1 P14S – Política de Retenção e Eliminação de Dados: define por quanto tempo os dados de cópia de segurança devem ser armazenados e eliminados de forma segura.

10.1.2 P13S – Política de Classificação e Rotulagem de Dados: ajuda a priorizar os dados que devem ser objeto de cópia de segurança com base nos níveis de classificação.

10.1.3 P30S – Política de Resposta a Incidentes: abrange os procedimentos caso as cópias de segurança falhem ou seja necessária a recuperação de dados após uma violação ou indisponibilidade de serviços.

10.1.4 P2S – Política de Papéis e Responsabilidades de Governação: atribui autoridade clara para a supervisão das cópias de segurança e a aplicação da política.

10.1.5 P17S – Política de Proteção de Dados e Privacidade: assegura que o tratamento de dados pessoais em cópias de segurança está alinhado com requisitos legais e de privacidade.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1: planeamento operacional e controlo dos sistemas de cópia de segurança como parte do SGSI

11.2 ISO/IEC 27002

11.2.1 Controlo 8.13: prescreve boas práticas para o agendamento, a monitorização e o restauro de cópias de segurança

11.2.2 Anexo A, Controlo 5.29: integração das cópias de segurança com a continuidade do negócio e a capacidade de restauro

11.3 NIST SP 800-53 Rev.

11.3.1 CP-9 (Planeamento de contingência): define estratégias estruturadas de cópia de segurança para a resiliência do negócio

11.3.2 MP-6 (Proteção de suportes): exige o tratamento e a destruição seguros dos suportes de cópia de segurança

11.4 RGPD da UE

11.4.1 Artigo 5(1)(f): exige a integridade e disponibilidade dos dados pessoais

11.4.2 Artigo 32(1)(c): exige a capacidade de restabelecer o acesso aos dados pessoais de forma atempada

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(c): exige cópias de segurança e recuperação como parte do planeamento da resiliência e da continuidade

11.6 DORA da UE

11.6.1 Artigo 10(1): as organizações do setor financeiro devem assegurar cópias de segurança como parte das medidas de continuidade das TIC

11.7 COBIT 2019

11.7.1 BAI04.05: exige estratégias de cópia de segurança documentadas

11.7.2 DSS04.07: destaca os testes regulares e o controlo dos processos de cópia de segurança e recuperação de dados