					Insira aqui a designação da entidade jurídica registada							
Número do documento: P15					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	Cláusulas 6.1.3, 8	Tratamento de riscos, planeamento e controlos operacionais de cópias de segurança
ISO/IEC 27002:2022	Controlos 8.13, 5.28, 5.29	Gestão de cópias de segurança, eliminação segura e resiliência
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Requisitos de cópia de segurança de sistemas, recuperação e sanitização de suportes
RGPD da UE	Artigo 32, Considerando 49	Restabelecimento e disponibilidade de dados pessoais, continuidade do negócio
Diretiva NIS2 da UE	Artigo 21(2)(c-e)	Controlos de cópias de segurança e continuidade para a resiliência
DORA da UE	Artigos 10, 11	Requisitos de cópias de segurança, recuperação e testes no setor financeiro
COBIT 2019	DSS01, DSS04, MEA03	Operações de cópias de segurança, continuidade e monitorização da conformidade

1. Finalidade

1.1 A finalidade desta política é definir os requisitos obrigatórios para a realização de cópias de segurança e o restauro de dados, sistemas e aplicações, de modo a suportar a resiliência operacional, a integridade dos dados e a continuidade do negócio.

1.2 A política estabelece um quadro normalizado para:

1.2.1 Proteger os dados da organização contra perdas resultantes de eliminação, corrupção, falhas ou ciberataques

1.2.2 Definir expectativas de recuperação através de parâmetros claros de RTO (Recovery Time Objective) e RPO (Recovery Point Objective)

1.2.3 Integrar as operações de cópia de segurança com o SGSI e com os Planos de Continuidade do Negócio e de Recuperação de Desastre (BCP/DRP)

1.2.4 Assegurar o cumprimento das leis aplicáveis e dos regulamentos setoriais em matéria de disponibilidade e recuperabilidade

1.3 A política aplica os controlos da ISO/IEC 27001:2022 relacionados com eliminação segura de dados (5.28), resiliência (5.29) e recuperação operacional (8.13), e está alinhada com as melhores práticas da ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, RGPD da UE, DORA da UE e Diretiva NIS2 da UE.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os sistemas operacionais e críticos para o negócio incluídos no âmbito do SGSI

2.1.2 Todos os dados empresariais estruturados e não estruturados, incluindo bases de dados, ficheiros, mensagens de correio eletrónico e configurações

2.1.3 Todos os ambientes — on-premises, na nuvem, híbridos e de armazenamento remoto/fora das instalações

2.1.4 Todo o pessoal responsável por gerir, executar, verificar ou restaurar processos de cópia de segurança

2.2 Aplica-se igualmente a:

2.2.1 Suportes e infraestrutura de cópia de segurança, incluindo fitas físicas, appliances virtuais, snapshots de disco e soluções de cópia de segurança alojadas na nuvem

2.2.2 Prestadores de serviços terceiros contratados para alojar, gerir ou tratar cópias de segurança da organização

2.2.3 Cópias de segurança de logs, configurações, rastos de auditoria e documentação operacional crítica para a continuidade

2.3 Os sistemas explicitamente excluídos de cópia de segurança devem ser documentados, sujeitos a análise de risco e formalmente aceites pelo Gestor do SGSI e pelo Proprietário do sistema.

3. Objetivos

3.1 Assegurar que todos os sistemas e dados críticos são objeto de cópia de segurança fiável, com frequência, redundância e controlos de segurança suficientes.

3.2 Disponibilizar mecanismos de restauro que cumpram os objetivos definidos de RTO e RPO, em alinhamento com as análises de impacto no negócio.

3.3 Manter documentação completa dos procedimentos de cópia de segurança, calendários de retenção, funções e tecnologias.

3.4 Validar a eficácia das operações de cópia de segurança através de testes sistemáticos de restauro, registo de falhas e acompanhamento das ações de remediação.

3.5 Proteger os dados de cópia de segurança contra acesso não autorizado, modificação ou destruição ao longo de todo o seu ciclo de vida.

3.6 Permitir o cumprimento de:

3.6.1 Requisitos operacionais e de continuidade da ISO/IEC 27001

3.6.2 Famílias CP e MP do NIST SP 800-53 para cópias de segurança e sanitização

3.6.3 Artigo 32 e Considerando 49 do RGPD da UE para o restabelecimento do acesso a dados pessoais

3.6.4 Artigo 10 do DORA da UE e Artigo 21 da Diretiva NIS2 da UE para continuidade e resiliência das TIC

3.7 Assegurar que os serviços de cópia de segurança prestados por terceiros cumprem as obrigações contratuais e regulamentares de segurança, incluindo cifragem, eliminação e protocolos de notificação.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova esta política e assegura que os sistemas críticos para o negócio são adequadamente protegidos por práticas aprovadas de cópia de segurança e restauro.

4.1.2 É responsável por assegurar que as operações de cópia de segurança dispõem de recursos adequados e são periodicamente revistas quanto à conformidade regulamentar.

4.2 Diretor de Segurança da Informação (CISO)

4.2.1 É responsável por esta política e assegura o alinhamento com os quadros mais abrangentes de segurança da informação, risco e continuidade.

4.2.2 Supervisiona a integração dos procedimentos de cópia de segurança no BCP/DRP, na resposta a incidentes e no planeamento da resiliência.

4.2.3 Revê as exceções de cópia de segurança e avalia propostas de aceitação do risco para exclusões de sistemas críticos.

[... 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, ou mais cedo se tal for desencadeado por:

9.1.1 Alterações na estratégia de continuidade do negócio ou de recuperação em caso de desastre

9.1.2 Novas obrigações regulamentares ou legais que afetem a frequência das cópias de segurança ou a retenção de dados

9.1.3 Alterações na arquitetura dos sistemas, nas ferramentas de cópia de segurança ou nos prestadores de serviços

9.1.4 Incidentes significativos ou constatações de auditoria relacionadas com perda de dados ou falhas de recuperação

9.2 A revisão deve ser coordenada pelo Diretor de Segurança da Informação em colaboração com:

9.2.1 Infraestrutura e Operações de TI

9.2.2 Auditoria Interna

9.2.3 Encarregado da Proteção de Dados (EPD)

9.2.4 Equipas de Continuidade do Negócio e Recuperação em caso de Desastre

9.3 Os calendários de cópia de segurança, listas de inclusão de sistemas, documentação de restauro e registos de exceções devem ser revistos em paralelo para assegurar:

9.3.1 Exatidão da cobertura de cópia de segurança para todos os ativos críticos

9.3.2 Cumprimento dos requisitos de RTO/RPO e retenção

9.3.3 Integridade dos logs de teste e dos relatórios de incidentes

9.3.4 Correção das lacunas de controlo anteriormente identificadas

9.4 Todas as atualizações devem:

9.4.1 Estar sujeitas a controlo de versões e ser retidas no repositório documental do SGSI

9.4.2 Incluir um resumo das alterações e a respetiva justificação

9.4.3 Ser aprovadas pela Alta Direção

9.4.4 Ser comunicadas a todo o pessoal técnico e de negócio impactado

10. Políticas relacionadas e interdependências

10.1 Esta política suporta diretamente e interage com os seguintes documentos relacionados:

10.1.1 P6 - Política de Gestão de Riscos: Identifica a priorização, com base no risco, da proteção por cópia de segurança de sistemas e serviços.

10.1.2 P12 - Política de Gestão de Ativos: Assegura que os sistemas elegíveis para cópia de segurança constam do inventário e estão associados ao acompanhamento do ciclo de vida e à classificação.

10.1.3 P13 - Política de Classificação e Rotulagem de Dados: Orienta quais as categorias de dados que exigem cópia de segurança, incluindo metadados de rotulagem para priorização.

10.1.4 P14 - Política de Retenção e Eliminação de Dados: Coordena a retenção das cópias de segurança com os limites regulamentares de retenção e a eliminação adequada de suportes expirados.

10.1.5 P16 - Política de Mascaramento de Dados e Pseudonimização: Suporta a minimização de dados durante a cópia de segurança de conjuntos de dados sensíveis.

10.1.6 P30 - Política de Resposta a Incidentes: É acionada em caso de falhas de cópia de segurança, problemas de restauro ou comprometimento de repositórios de dados de cópia de segurança.

10.2 Estas políticas interligadas formam um quadro coeso que assegura que a governação das cópias de segurança está integrada no SGSI mais abrangente da organização e na sua estratégia de resiliência operacional.

11. Normas e quadros de referência

11.1 ISO/IEC 27001:

11.1.1 Cláusula 6.1.3 - Plano de tratamento de riscos: Suporta a priorização das cópias de segurança com base no risco e o planeamento do restauro.

11.1.2 Cláusula 8.1 - Planeamento e controlo operacional: Integra controlos de recuperação e continuidade como parte das salvaguardas operacionais.

11.1.3 Controlo 5.28 do Anexo A - Eliminação segura ou reutilização de equipamentos: Aborda a sanitização segura de suportes de cópia de segurança.

11.1.4 Controlo 5.29 do Anexo A - Segurança da informação durante interrupções: Assegura capacidades de restauro durante incidentes ou desastres.

11.1.5 Controlo 8.13 do Anexo A - Cópia de segurança da informação: Diretamente tratado através de operações de cópia de segurança calendarizadas, testadas e seguras.

11.2 ISO/IEC 27002:2022 - Controlos 8.13, 5.28, 5.29: Estes controlos reforçam o requisito de cópias de segurança regulares, validação da integridade e planeamento do restauro em todos os ambientes de TI.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Cópia de segurança de sistemas: Estabelece procedimentos abrangentes de cópia de segurança, incluindo armazenamento fora das instalações e testes de restauro.

11.3.2 CP-10 - Recuperação e restauro de sistemas: Exige procedimentos validados para restauro total ou parcial em alinhamento com os objetivos de recuperação.

11.3.3 MP-6 - Sanitização de suportes: Assegura o tratamento seguro de suportes de cópia de segurança obsoletos.

11.3.4 SI-12 - Procedimentos de tratamento da informação: Reforça as responsabilidades de cópia de segurança e recuperação para dados sensíveis.

11.4 RGPD da UE (2016/679):

11.4.1 Artigo 32 - Segurança do tratamento: Impõe capacidades de restauro e salvaguardas de disponibilidade dos dados, em especial no caso de dados pessoais.

11.4.2 Considerando 49: Suporta medidas de continuidade do negócio e recuperação em caso de desastre, incluindo cópia de segurança segura como parte da resiliência organizacional.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 Artigo 21(2)(c-e): Exige medidas técnicas e organizativas, incluindo controlos de cópia de segurança e continuidade, para assegurar a resiliência dos serviços.

11.6 DORA da UE (2022/2554):

11.6.1 Artigo 10 - Continuidade do negócio das TIC: Exige que as entidades financeiras disponham de cópia integral de segurança dos dados, recuperação e planeamento de continuidade.

11.6.2 Artigo 11 - Testes dos Planos de Continuidade do Negócio das TIC: Enfatiza a validação da capacidade de recuperação através de testes regulares.

11.7 COBIT 2019:

11.7.1 DSS01 - Operações geridas: Suporta a prestação fiável de serviços através da proteção da disponibilidade dos dados.

11.7.2 DSS04 - Continuidade gerida: Define controlos estratégicos e operacionais de continuidade, incluindo cópias de segurança verificadas.

11.7.3 MEA03 - Monitorizar, avaliar e analisar a conformidade: Exige revisão periódica das medidas de continuidade, incluindo a eficácia dos controlos de cópia de segurança.