					Insira aqui a designação da entidade jurídica registada							
Número do documento: P05					Título do documento: **Política de Gestão de Alterações**							
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 aplicáveis

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 6.1, 5.15	Aborda ações relativas a riscos, controlo de acesso e gestão de alterações
ISO/IEC 27002:2022	Controlo 8.32	Implementa um processo estruturado de gestão de alterações
NIST SP 800-53 Rev.5	CM-2 a CM-14	Controlos de gestão da configuração
RGPD da UE	Artigos 32(1)(b–d), 25; Considerando 78	Medidas técnicas e organizativas para a segurança de sistemas e dados durante alterações
Diretiva NIS2 da UE	Artigo 21(2)(a, b, d, e)	Exige a gestão do risco associado a alterações de TIC
DORA da UE	Artigos 5, 8, 12	Regula o risco operacional e de TIC, bem como a notificação de incidentes
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Estrutura o desempenho, a conformidade e os requisitos da gestão de alterações de TI

1. Finalidade

1.1. Esta política estabelece um quadro formal para iniciar, avaliar, aprovar, implementar e rever alterações aos sistemas de informação, à infraestrutura, às aplicações e aos processos relacionados da organização.

1.2. Assegura que todas as alterações são executadas de forma controlada e auditável, minimizando o risco de interrupção, comprometimento da segurança ou incumprimento regulamentar.

1.3. Suporta o Controlo 8.32 do Anexo A da ISO/IEC 27001:2022, impondo práticas de gestão de alterações seguras, documentadas e alinhadas com o risco.

1.4. A política assegura igualmente a rastreabilidade das decisões de alteração e promove a resiliência operacional durante alterações planeadas ou de emergência.

2. Âmbito

2.1. Esta política aplica-se a todas as alterações que afetem sistemas, dados e ambientes no âmbito do SGSI, incluindo:

2.1.1. Infraestrutura de TI (on-premises, cloud, híbrida)

2.1.2. Ambientes de produção, pré-produção e recuperação de desastre

2.1.3. Aplicações de negócio, serviços, APIs e integrações

2.1.4. Definições de configuração, aplicação de patches, lançamentos de software e migrações de sistemas

2.1.5. Correções de emergência e alterações planeadas ou baseadas em projeto

2.2. Regula as alterações iniciadas por:

2.2.1. Pessoal interno (operações de TI, programadores, proprietários de sistemas)

2.2.2. Fornecedores externos, prestadores de serviços geridos (MSP) e contratados

2.2.3. Equipas de projeto durante a implementação de sistemas, atualizações ou transições de serviço

2.3. Esta política não se aplica a:

2.3.1. Ambientes temporários de teste e desenvolvimento sem acesso a dados de produção

2.3.2. Configurações pessoais de utilizador (abrangidas pela Política de Utilização Aceitável)

2.3.3. Alterações a sistemas fora do perímetro de controlo da organização, exceto quando afetem ativos integrados ou obrigações de conformidade

3. Objetivos

3.1. Assegurar que todas as alterações são revistas, aprovadas, testadas e documentadas antes da execução.

3.2. Manter a disponibilidade dos sistemas, a integridade dos dados e a continuidade do serviço durante e após as atividades de alteração.

3.3. Exigir classificações de alteração definidas, planos de reversão e avaliações de risco para todos os tipos de alteração.

3.4. Permitir a tomada de decisão transparente e o escalonamento através de uma governação estruturada.

3.5. Apoiar a demonstração de conformidade em auditoria através de registos de alterações rastreáveis e revisões pós-implementação.

3.6. Impor a segregação de funções e reduzir o risco de alterações não autorizadas ou conflituantes em sistemas críticos.

4. Papéis e responsabilidades

4.1. Alta Direção

4.1.1. Aprova a P05 Política de Gestão de Alterações e assegura o alinhamento com os objetivos estratégicos e as obrigações regulamentares.

4.1.2. Aprova programas de alteração de elevado impacto ou transversais às funções no âmbito da supervisão de governação.

4.1.3. Afeta os recursos e o orçamento necessários para ferramentas de controlo de alterações e formação do pessoal.

4.2. Conselho Consultivo de Alterações (CAB)

4.2.1. Revê e autoriza alterações padrão e alterações de maior impacto, assegurando a adequada avaliação do risco, impacto e dependências.

4.2.2. Valida planos de reversão, resultados dos testes, comunicações às partes interessadas e calendarização.

4.2.3. É composto por proprietários de sistemas, segurança, operações de TI, responsáveis de negócio e representantes de conformidade.

4.2.4. Pode delegar decisões relativas a alterações de baixo risco ou alterações de emergência em condições documentadas.

[... 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. Desencadeadores e periodicidade de revisão

9.1.1. Esta política deve ser revista anualmente ou quando ocorrer:

9.1.1.1. Alterações significativas de TI ou de infraestrutura

9.1.1.2. Incidentes significativos relacionados com alterações falhadas ou não autorizadas

9.1.1.3. Atualizações regulamentares ou novas obrigações legais relacionadas com alterações

9.1.1.4. Implementação de novas ferramentas ou plataformas CMS

9.2. Processo de revisão da Política de Gestão de Alterações

9.2.1. O Gestor de Alterações liderará o processo de revisão em colaboração com:

9.2.1.1. TI, Segurança e Operações

9.2.1.2. Auditoria Interna e Gestão de Risco

9.2.1.3. Representantes do CAB

9.2.2. As atualizações devem ser revistas e aprovadas pela Alta Direção e pelo Comité de Direção do SGSI.

9.2.3. As versões reemitidas devem ser controladas no Registo de Documentos e comunicadas às partes afetadas, com nova confirmação quando necessário.

9.3. Controlo documental e versionamento

9.3.1. Todas as versões devem incluir:

9.3.1.1. ID da política, título e nível de classificação

9.3.1.2. Proprietário e histórico de revisões

9.3.1.3. Registo de alterações e data de entrada em vigor

9.3.1.4. Autoridade de aprovação

9.3.2. As versões arquivadas devem ser retidas de acordo com a Política de Retenção de Documentos (mínimo de 3 anos).

10. Políticas relacionadas e ligações

10.1. Esta política está diretamente ligada às seguintes políticas e apoia a respetiva aplicação:

10.1.1. P1 – Política de Segurança da Informação: Estabelece o requisito de controlos formais de segurança e responsabilização ao nível do processo, incluindo a governação da gestão de alterações.

10.1.2. P2 – Política de Papéis e Responsabilidades de Governação: Define as autoridades de aprovação e a segregação de funções relevantes para a autorização e supervisão de alterações.

10.1.3. P4 – Política de Controlo de Acesso: Assegura que as permissões de acesso de implementadores e revisores de alterações seguem o princípio do menor privilégio.

10.1.4. P6 – Política de Gestão de Risco: Assegura que todas as alterações estão sujeitas a avaliação de risco adequada e a estratégias de mitigação.

10.1.5. P33 – Política de Monitorização de Auditoria e Conformidade: Regula a validação e a revisão de auditoria dos registos de gestão de alterações e das violações.

10.2. Estas políticas, em conjunto, permitem um ciclo de vida de gestão de alterações defensável, rastreável e seguro no âmbito do quadro do SGSI.

11. Normas e referenciais aplicáveis

11.1. ISO/IEC 27001:2022

11.1.1. Cláusula 6.1 – Ações para tratar riscos e oportunidades: Esta política apoia a identificação, avaliação e controlo dos riscos relacionados com alterações.

11.1.2. Cláusula 5.15 – Controlo de acesso: Assegura que o acesso durante as alterações é controlado e rastreável.

11.1.3. Controlo 8.32 do Anexo A – Gestão de alterações: Esta política implementa integralmente o requisito de gerir alterações a instalações e sistemas de processamento da informação de forma planeada e controlada.

11.2. ISO/IEC 27002:2022 – Controlo 8.32

11.2.1. Reforça a implementação de um processo estruturado de gestão de alterações, incluindo classificação de alterações, aprovação, testes, reversão e documentação.

11.3. NIST SP 800-53 Rev.5

11.3.1. Família CM (CM-1 a CM-14): Esta política está fortemente alinhada com os controlos de gestão da configuração, incluindo configurações de referência (CM-2), controlo de alterações de configuração (CM-3), análise de impacto na segurança (CM-4) e restrições de acesso (CM-5).

11.3.2. Família AU (AU-2, AU-6, AU-12): Os mecanismos de registo e auditoria referidos nesta política suportam a rastreabilidade de eventos e a revisão de conformidade das atividades relacionadas com alterações.

11.3.3. RA-3, RA-5: As avaliações de risco orientadas por alterações e os varrimentos de vulnerabilidades estão integrados no processo de avaliação de alterações.

11.3.4. PM-11 (Definição de Missão/Processo de Negócio): Assegura que a continuidade do negócio e os objetivos operacionais são preservados durante as alterações.

11.4. RGPD da UE (2016/679)

11.4.1. Artigo 32(1)(b–d): Esta política apoia o requisito de medidas técnicas e organizativas adequadas para garantir a segurança dos dados, especialmente durante alterações de sistema.

11.4.2. Artigo 25 – Proteção de dados desde a conceção e por defeito: Assegura que as alterações que afetam dados pessoais integram privacidade e segurança na conceção e na implementação.

11.4.3. Considerando 78: Exige que os responsáveis pelo tratamento implementem mecanismos, tais como políticas de controlo de alterações, para assegurar a confidencialidade, integridade e resiliência contínuas dos sistemas de tratamento.

11.5. Diretiva NIS2 da UE (2022/2555)

11.5.1. Artigo 21(2)(a, b, d, e): Exige medidas técnicas e organizativas para gerir riscos de TIC, incluindo os decorrentes de alterações de sistemas, atualizações de software e modificações de infraestrutura.

11.6. DORA da UE (2022/2554)

11.6.1. Artigo 5 – Quadro de governação e controlo interno: Esta política impõe princípios de gestão do risco operacional associados a alterações e atualizações de TIC.

11.6.2. Artigo 8 – Quadro de gestão do risco de TIC: Exige que as entidades financeiras gerem todas as alterações com impacto nos sistemas de TIC através de processos estruturados de gestão de alterações, refletidos nesta política nas exigências de classificação, testes, reversão e documentação.

11.6.3. Artigo 12 – Notificação de incidentes: Assegura que alterações falhadas que conduzam a perturbações de TIC são rastreáveis, documentadas e reportadas quando aplicável.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: Esta política cumpre diretamente os objetivos do BAI06 ao estabelecer fluxos de trabalho estruturados para aprovação de alterações, avaliação de impacto, comunicação e testes.

11.7.2. BAI02 – Managed Requirements Definition e BAI03 – Managed Solutions Identification and Build: Asseguram que alterações orientadas pelo negócio são revistas e implementadas de forma segura.

11.7.3. DSS01 – Managed Operations: Apoia a integridade contínua dos sistemas durante a execução de alterações.

11.7.4. MEA01 e MEA03 – Monitor, Evaluate, and Assess Performance and Compliance: Permite a supervisão contínua da eficácia e da aplicação da política de gestão de alterações.