					Insira aqui a designação da entidade jurídica registada							
Número do documento: P05S					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

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 6.1, 8	
ISO/IEC 27002:2022	Controlo 8	
NIST SP 800-53 Rev. 5	CM-2 a CM-5, CM-11	
Diretiva NIS2 da UE	Artigo 21(2)(b)	
DORA da UE	Artigos 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Finalidade

1.1 Esta política assegura que todas as alterações a sistemas de TI, configurações, aplicações de negócio ou serviços na nuvem são planeadas, sujeitas a avaliação de risco, testadas e aprovadas antes da implementação.

1.2 O objetivo é reduzir interrupções operacionais, riscos de segurança e indisponibilidades de serviço, através do estabelecimento de um processo simplificado, mas aplicável, adequado mesmo a pequenas empresas com recursos limitados.

1.3 Esta política apoia a certificação ISO/IEC 27001:2022 ao formalizar a forma como as alterações técnicas e operacionais são geridas e documentadas.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Trabalhadores e responsáveis departamentais que proponham ou executem alterações

2.1.2 Prestadores externos de serviços de TI que gerem sistemas ou software

2.1.3 Diretor-Geral (GM), que detém a responsabilidade global pela aprovação de alterações

2.2 Abrange alterações a:

2.2.1 Software (atualizações, patches, novas aplicações)

2.2.2 Hardware (substituições, atualizações)

2.2.3 Configurações de rede e de firewall

2.2.4 Serviços na nuvem, permissões de acesso de utilizadores ou integrações com fornecedores

2.2.5 Alterações a processos de negócio críticos que envolvam sistemas de informação

2.3 Tanto as alterações planeadas como as alterações de emergência estão incluídas no âmbito desta política.

3. Objetivos

3.1 Assegurar que todas as alterações a sistemas de TI e processos de negócio são autorizadas, documentadas e reversíveis caso ocorram problemas.

3.2 Prevenir indisponibilidades não planeadas, perda de dados ou incidentes de segurança causados por alterações não controladas.

3.3 Definir procedimentos simples e repetíveis para submissão, aprovação, testes e reversão de alterações.

3.4 Manter um registo de alterações auditável que suporte a responsabilização operacional e a conformidade regulamentar.

3.5 Permitir a tomada de decisão baseada no risco para alterações significativas ou sensíveis.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Detém a responsabilidade final por todas as alterações de maior relevância.

4.1.2 Revê e aprova alterações não rotineiras, críticas ou de risco elevado.

4.1.3 Revê o registo de alterações trimestralmente ou após incidentes significativos.

4.2 Suporte de TI ou prestador externo de serviços de TI

4.2.1 Implementa alterações, incluindo atualizações de configuração, aplicação de patches e migrações de sistemas.

4.2.2 Mantém um registo básico de alterações com datas, tipos de alteração, resultados e aprovadores.

4.2.3 Testa as alterações antes da implementação e aplica os procedimentos de reversão sempre que necessário.

4.2.4 Notifica os utilizadores afetados antes e depois de alterações de maior impacto.

[... 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

9.1.1 Esta política deve ser revista anualmente pelo Diretor-Geral (GM) ou pelo responsável de TI designado, para assegurar o alinhamento com os sistemas, fluxos de trabalho e requisitos regulamentares em vigor.

9.2 Revisões intercalares

9.2.1 As revisões devem também ser desencadeadas por:

9.2.1.1 Incidentes de segurança causados por gestão inadequada de alterações

9.2.1.2 Introdução de novos sistemas de TI

9.2.1.3 Alterações a normas relevantes como ISO, NIS2 ou DORA

9.3 Documentação das atualizações

9.3.1 As alterações a esta política devem estar sujeitas a controlo de versões e ser aprovadas pelo Diretor-Geral (GM). Cada versão deve registar a data, o resumo das alterações e o aprovador.

9.4 Comunicação da política

9.4.1 Quaisquer atualizações devem ser comunicadas a todos os trabalhadores e prestadores externos afetados. A documentação deve ser atualizada em todos os locais de referência (por exemplo, portal de colaboradores, unidades partilhadas).

10. Políticas relacionadas e ligações

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

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: Define a autoridade de aprovação para alterações.

10.1.2 P4S – Política de Controlo de Acessos: Assegura que as alterações aos acessos resultantes de alterações são documentadas e implementadas corretamente.

10.1.3 P7S – Política de Admissão e Cessação: Coordena alterações relacionadas com transições de função e atribuição de acessos.

10.1.4 P15S – Política de Cópias de Segurança e Restauro: Assegura que os procedimentos de reversão e recuperação podem ser executados se uma alteração falhar.

10.1.5 P30S – Política de Resposta a Incidentes: Estabelece a forma como alterações falhadas ou não autorizadas são tratadas como incidentes de segurança.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – O planeamento baseado no risco deve incluir atividades de alteração.

11.1.2 Cláusula 8.1 – Os controlos operacionais devem ser aplicados de forma consistente às atividades relacionadas com alterações para assegurar a integridade do serviço.

11.2 ISO/IEC 27002

11.2.1 Controlo 8.32 – Fornece orientações para processos seguros de gestão de alterações, incluindo documentação, testes e aprovação.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Configuração de referência para sistemas antes da alteração.

11.3.2 CM-3 – Controlo de alterações de configuração.

11.3.3 CM-4 – Análise do impacto na segurança.

11.3.4 CM-5 – Aprovação e documentação de alterações.

11.3.5 CM-11 – Auditoria e monitorização de alterações.

11.4 Diretiva NIS2 da UE

11.4.1 Artigo 21(2)(b) – Exige procedimentos formais para medidas técnicas e organizativas de segurança, incluindo a gestão de alterações.

11.5 DORA da UE

11.5.1 Artigos 6(9) e 8(4)(b) – Exigem que as entidades financeiras mantenham processos de gestão de alterações e de gestão da configuração para sistemas de TIC.

11.6 COBIT 2019

11.6.1 BAI06 – Gerir Alterações: Dá ênfase ao planeamento, à avaliação de riscos e às capacidades de reversão.

11.6.2 DSS01 – Gerir Operações: Assegura a integridade operacional durante transições técnicas e alterações.