					Insira aqui a designação da entidade jurídica registada							
Número do documento: P37S					Título do documento: **Política de Conformidade Legal e Regulamentar**							
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 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controlo 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
RGPD da UE	Artigos 5, 6, 32, 33	
Diretiva NIS2 da UE	Artigos 21(2)(a), 21(2)(f), 23	
DORA da UE	Artigos 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Finalidade

1.1 Esta política define a abordagem da organização para identificar, cumprir e demonstrar o cumprimento das obrigações legais, regulamentares e contratuais.

1.2 Estabelece responsabilidades claras e medidas práticas para apoiar a organização no cumprimento das suas obrigações, incluindo legislação de proteção de dados, referenciais de cibersegurança, acordos com clientes e normas de certificação.

1.3 Assegura que, mesmo sem uma função de conformidade dedicada, a organização consegue manter operações juridicamente sólidas, responder adequadamente a incidentes e manter a preparação para auditorias.

1.4 Esta política é essencial para viabilizar a certificação ISO/IEC 27001:2022 e satisfazer as expectativas externas de clientes, reguladores e parceiros.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os trabalhadores, contratados, prestadores de serviços independentes e fornecedores terceiros.

2.1.2 Todos os serviços, operações, sistemas e atividades de tratamento de dados em que a organização tenha de cumprir requisitos legais ou contratuais.

2.1.3 Todos os locais e dispositivos utilizados para tratar informação da organização, quer em escritório, em regime remoto ou alojados na nuvem.

2.2 A política abrange:

2.2.1 Legislação de proteção de dados, como o RGPD da UE.

2.2.2 Regulamentação de cibersegurança, como a Diretiva NIS2 da UE.

2.2.3 Obrigações específicas do setor, quando aplicável.

2.2.4 Contratos com clientes, acordos de confidencialidade (NDA) e cláusulas de auditoria.

2.2.5 Certificações voluntárias (por exemplo, ISO 27001) e políticas internas que devam ser aplicadas para assegurar o cumprimento.

3. Objetivos

3.1 Estabelecer responsabilização: atribuir responsabilidades claras pela monitorização, atualização e aplicação das obrigações legais, regulamentares e contratuais.

3.2 Proteger a organização: minimizar o risco de infrações legais, coimas, violações de dados e danos reputacionais.

3.3 Assegurar a preparação para auditorias: manter registos verificáveis que demonstrem como a organização cumpre as suas obrigações de conformidade.

3.4 Apoiar a integração das políticas: assegurar que os deveres legais e regulamentares são aplicados de forma consistente em todas as políticas e processos.

3.5 Gerir exceções com transparência: assegurar que quaisquer exceções de conformidade são documentadas, justificadas e aprovadas, de modo a evitar responsabilidade legal.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Detém a responsabilidade global pelo cumprimento legal e regulamentar da organização.

4.1.2 Mantém o Registo de Conformidade e assegura que este permanece atualizado.

4.1.3 Revê os contratos com clientes e assegura que as obrigações específicas são acompanhadas e aplicadas.

4.1.4 Aprova exceções a obrigações de conformidade apenas quando sejam legalmente justificáveis e existam controlos compensatórios.

4.2 Assessores externos (por exemplo, consultores jurídicos, de TI ou de conformidade)

4.2.1 Apoiam o GM na identificação da legislação, certificações e obrigações aplicáveis (por exemplo, RGPD, NIS2, ISO 27001).

4.2.2 Prestam orientação sobre a interpretação de novos regulamentos ou de alterações à legislação em vigor.

4.2.3 Podem apoiar na atualização de políticas, em auditorias ou na resposta a violações, quando exista exposição jurídica.

[... 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 programada

9.1.1 Esta política deve ser revista a cada 12 meses pelo GM.

9.1.2 A revisão deve confirmar:

9.1.2.1 A relevância para o contexto legal e contratual em vigor.

9.1.2.2 O correto reflexo dos acordos com clientes e das obrigações de serviço.

9.1.2.3 O alinhamento com o Registo de Conformidade e com as restantes políticas.

9.2 Atualizações desencadeadas por eventos

9.2.1 É obrigatória uma revisão imediata se:

9.2.1.1 Uma nova lei ou regulamento passar a ser aplicável (por exemplo, nova regra de proteção de dados).

9.2.1.2 Um cliente adicionar requisitos de conformidade complexos ao seu acordo.

9.2.1.3 Ocorrer uma violação ou incidente de incumprimento.

9.2.1.4 A organização expandir a sua atividade para um mercado ou setor regulado.

9.3 Aprovação das atualizações e controlo de versões

9.3.1 Todas as atualizações devem ser documentadas, sujeitas a controlo de versões e aprovadas pelo GM.

9.3.2 As versões históricas devem ser mantidas para fins de auditoria e efeitos legais.

9.4 Comunicação de alterações

9.4.1 Os trabalhadores e prestadores de serviços devem ser informados das alterações às políticas no prazo de 5 dias úteis após a aprovação.

9.4.2 Quaisquer fornecedores afetados devem igualmente confirmar os termos atualizados antes de continuarem a prestação do serviço.

10. Políticas relacionadas e ligações

10.1 Esta política é suportada e aplicada através das seguintes políticas SME:

10.1.1 P3S – Política de Utilização Aceitável: previne comportamentos que possam violar requisitos legais ou contratuais (por exemplo, partilha não autorizada de ficheiros).

10.1.2 P8S – Política de Sensibilização e Formação em Segurança da Informação: sensibiliza os trabalhadores para as obrigações de conformidade e para a forma de evitar violações.

10.1.3 P14S – Política de Retenção e Eliminação de Dados: assegura práticas lícitas de tratamento de dados ao longo do ciclo de vida dos dados.

10.1.4 P17S – Política de Proteção de Dados e Privacidade: cumpre os requisitos do RGPD e os requisitos dos clientes em matéria de tratamento de dados.

10.1.5 P30S – Política de Resposta a Incidentes: define a forma de responder a violações de dados ou falhas de conformidade, incluindo os prazos de notificação.

10.1.6 P36S – Política de Redes Sociais e Comunicações Externas: assegura que as comunicações públicas não violam obrigações legais ou regulamentares.

10.2 Cada política associada aplica uma parte do quadro de conformidade legal e deve ser implementada de forma articulada.

11. Normas e referenciais de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – Ações para tratar riscos e oportunidades: inclui riscos de conformidade.

11.1.2 Cláusula 8.1 – Planeamento e controlo operacional: exige a execução de processos que cumpram requisitos legais e contratuais.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.36 – Orienta a organização na manutenção de registos de obrigações e na garantia de respostas adequadas às necessidades legais e regulamentares.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Política e procedimentos: exige políticas formais de conformidade.

11.3.2 PM-1 – Plano do programa de segurança da informação: exige a integração da conformidade legal no planeamento da segurança.

11.3.3 CA-1 – Avaliação, autorização e monitorização.

11.3.4 AU-1 – Política de auditoria: exige a manutenção de evidência de conformidade.

11.4 RGPD da UE

11.4.1 Artigo 5 – Princípios do tratamento de dados, incluindo a responsabilização.

11.4.2 Artigo 6 – Fundamento de licitude para o tratamento.

11.4.3 Artigo 32 – Segurança do tratamento.

11.4.4 Artigo 33 – Notificação de violação no prazo de 72 horas.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(a) e (f) – Políticas internas para controlo do risco e conformidade regulamentar.

11.5.2 Artigo 23 – Aplicação e penalizações por falhas de conformidade.

11.6 Regulamento DORA da UE

11.6.1 Artigo 5(2) – Supervisão da gestão do risco das TIC.

11.6.2 Artigo 9(1) – Governação interna da conformidade.

11.6.3 Artigo 17 – Acordos contratuais com prestadores de serviços TIC.

11.7 COBIT 2019

11.7.1 APO12 – Risco gerido: assegura que os riscos de conformidade são acompanhados e tratados.

11.7.2 APO13 – Segurança gerida: abrange a aplicação, com base no risco, da conformidade regulamentar e contratual.

11.7.3 DSS01 – Operações geridas: exige capacidade operacional para cumprir obrigações legais.