					Insira aqui a designação da entidade jurídica registada							
Número do documento: P37					Título do documento: **Política de Cumprimento 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**

1. Finalidade

1.1 A presente política estabelece o quadro obrigatório para identificar, gerir e assegurar o cumprimento de todas as obrigações legais, regulamentares e contratuais relevantes para a segurança da informação, a privacidade dos dados e as funções operacionais da organização.

1.2 O objetivo é prevenir situações de incumprimento suscetíveis de resultar em coimas, responsabilidade legal, interrupção da atividade, danos reputacionais ou medidas regulatórias.

1.3 Esta política apoia a integração dos requisitos de conformidade na governação, na gestão do risco, nos fluxos de trabalho operacionais, nos ciclos de vida dos projetos e na conceção dos sistemas.

1.4 Assegura que todas as obrigações relevantes — em diferentes jurisdições, setores de atividade e âmbitos regulatórios — sejam claramente documentadas, avaliadas, monitorizadas e aplicadas em toda a organização.

2. Âmbito

2.1 Esta política aplica-se a todos os departamentos, funções, unidades de negócio e indivíduos que atuem em nome da organização, incluindo:

2.1.1 Trabalhadores permanentes e temporários

2.1.2 Prestadores de serviços, consultores e estagiários

2.1.3 Fornecedores terceiros, subcontratantes ou parceiros que tratem dados da organização, utilizem os seus sistemas ou assumam responsabilidades regulatórias

2.1.4 Qualquer processo de negócio, projeto ou iniciativa sujeito a controlo legal ou regulatório

2.2 Os domínios de conformidade abrangidos por esta política incluem, sem caráter limitativo:

2.2.1 Obrigações de segurança da informação e cibersegurança (por exemplo, ISO/IEC 27001, NIS2, DORA)

2.2.2 Legislação de proteção de dados e privacidade (por exemplo, RGPD, legislação setorial de privacidade)

2.2.3 Regulamentação setorial (por exemplo, financeira, da saúde, automóvel, defesa)

2.2.4 Obrigações contratuais decorrentes de acordos de confidencialidade (NDA), acordos de nível de serviço (SLA) ou acordos de tratamento de dados com terceiros

2.2.5 Requisitos legais relacionados com notificação de incidentes, interação com autoridades de aplicação da lei e transferência internacional de dados

3. Objetivos

3.1 Assegurar que todas as leis, regulamentos, normas e obrigações contratuais aplicáveis sejam identificados, documentados, interpretados e aplicados em toda a organização.

3.2 Integrar os requisitos legais e regulatórios no SGSI da organização, nos processos de gestão do risco, nos acordos com fornecedores e na conceção de produtos e serviços.

3.3 Disponibilizar um mecanismo de monitorização proativa da evolução regulatória e de atualização consequente dos controlos e da documentação.

3.4 Definir uma responsabilização clara pela supervisão da conformidade, pelo escalonamento de violações, pelo tratamento de exceções e pela comunicação externa.

3.5 Assegurar a auditabilidade e a defensabilidade da posição legal e regulatória da organização durante inspeções, investigações ou auditorias de certificação.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Detém a responsabilidade estratégica pelo alinhamento legal e regulatório em toda a organização.

4.1.2 Revê e aprova decisões de conformidade de elevado risco, incluindo aceitações de risco e litígios.

4.2 Responsável pela Conformidade / Assessoria Jurídica / Consultor Jurídico

4.2.1 Mantém o Registo de Obrigações de Conformidade, com a listagem de todas as leis, normas, certificações e cláusulas contratuais aplicáveis.

4.2.2 Realiza avaliações de impacto legal para novos serviços, mercados ou fluxos de dados.

4.2.3 Fornece interpretação autorizada de leis e normas.

[... 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 da política

9.1.1 Esta política deve ser revista pelo menos uma vez por ano civil para:

9.1.1.1 Assegurar o alinhamento contínuo com legislação atualizada, normas do setor e enquadramentos regulatórios

9.1.1.2 Validar a eficácia operacional com base nas constatações de auditoria e no histórico de incidentes

9.1.1.3 Refletir alterações organizacionais (por exemplo, novas jurisdições, sistemas ou linhas de negócio)

9.2 Revisões desencadeadas por evento

9.2.1 Devem ser iniciadas revisões intercalares quando:

9.2.2 Um novo requisito legal ou regulatório seja aprovado ou atualizado

9.2.3 Um incidente de conformidade ou uma auditoria revele insuficiências da política

9.2.4 A organização entre num novo mercado ou linha de serviço sujeita a enquadramentos de conformidade distintos

9.2.5 Tendências de supervisão regulatória ou orientações dos reguladores indiquem alterações na postura de risco

9.3 Titularidade e aprovação

9.3.1 O Departamento Jurídico e o Responsável pela Conformidade são conjuntamente responsáveis pela coordenação do processo de revisão.

9.3.2 As revisões finais da política devem ser aprovadas pela Alta Direção e registadas no Registo de Alterações à Política, com as respetivas referências de controlo de alterações e planos de comunicação.

9.4 Controlo de versões e comunicação

9.4.1 Qualquer versão atualizada desta política deve:

9.4.1.1 Incluir um resumo das principais alterações

9.4.1.2 Ser redistribuída através de canais oficiais (por exemplo, portal de políticas, LMS, boletins internos)

9.4.1.3 Exigir confirmação dos colaboradores afetados, em particular daqueles com funções jurídicas, operacionais, de segurança e de gestão de fornecedores

10. Políticas relacionadas e articulações

10.1 Esta política articula-se com as seguintes políticas do SGSI da organização e reforça-as:

10.1.1 P1 – Política de Segurança da Informação: Estabelece os princípios de governação de base que asseguram que todas as políticas de segurança da informação — incluindo as de

conformidade — estão alinhadas com os requisitos estratégicos do negócio e com os requisitos regulatórios.

10.1.2 P2 – Política de Papéis e Responsabilidades de Governação: Define as autoridades de decisão, incluindo os papéis jurídicos e de conformidade responsáveis pela supervisão regulatória e pela responsabilização.

10.1.3 P6 – Política de Gestão do Risco: Apoia a avaliação, a titularidade e a mitigação dos riscos de conformidade legal e regulatória em toda a organização.

10.1.4 P8 – Política de Sensibilização e Formação em Segurança da Informação: Assegura que todo o pessoal é informado das responsabilidades de conformidade e recebe formação adequada à função.

10.1.5 P12 – Política de Gestão de Ativos: Reforça as obrigações legais de gestão e proteção de ativos regulados ou contratuais, incluindo os que envolvem dados pessoais e infraestruturas críticas.

10.1.6 P30 – Política de Resposta a Incidentes: Rege as notificações legais obrigatórias (por exemplo, artigo 33 do RGPD) e os procedimentos de escalonamento em caso de violação de conformidade ou evento regulatório.

10.1.7 P33 – Política de Monitorização de Auditoria e Conformidade: Disponibiliza atividades estruturadas de garantia — incluindo testes aos controlos e recolha de evidência — necessárias para a verificação interna e externa da conformidade.

11. Normas e referenciais

11.1 ISO/IEC 27001

11.1.1 Cláusula 4.2 – Compreender as necessidades e expectativas das partes interessadas: Exige a identificação e a integração dos requisitos legais e regulatórios no SGSI.

11.1.2 Cláusula 5.1 – Liderança e compromisso: Determina a responsabilidade executiva pelo estabelecimento e manutenção do cumprimento legal em toda a organização.

11.1.3 Cláusula 5.3 – Papéis, responsabilidades e autoridades organizacionais: Assegura a clareza dos papéis em matéria de supervisão jurídica e conformidade regulatória.

11.1.4 Controlo 5.36 do Anexo A – Cumprimento de requisitos legais, estatutários, regulamentares e contratuais: Estabelece a obrigação de identificar e cumprir requisitos decorrentes de leis, regulamentos e contratos.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.36: Detalha orientações de implementação para manter um registo de obrigações de conformidade, validar requisitos regulatórios e assegurar uma retenção estruturada da evidência.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – Política e procedimentos de planeamento da segurança: Exige que os requisitos de conformidade sejam incorporados nas estruturas de governação e na documentação.

11.3.2 PM-1 – Plano do programa de segurança da informação: Determina os controlos regulatórios como componente do programa de segurança em sentido lato.

11.3.3 CA-7 – Monitorização contínua: Apoia a supervisão da eficácia dos controlos no cumprimento de requisitos legais e de política.

11.3.4 AU-9 – Proteção da informação de auditoria: Assegura que os registos e evidências de auditoria de conformidade são protegidos e disponibilizados para inspeção.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 5 – Princípios relativos ao tratamento de dados pessoais: Exige licitude, transparência e responsabilização.

11.4.2 Artigo 6 – Licitude do tratamento: Determina a existência de fundamentos de licitude adequados para todas as atividades de tratamento de dados.

11.4.3 Artigo 24 – Responsabilidade do responsável pelo tratamento: Estabelece responsabilidade direta por assegurar a conformidade regulatória.

11.4.4 Artigo 32 – Segurança do tratamento: Exige a implementação de medidas técnicas e organizativas adequadas.

11.4.5 Artigo 33 – Notificação de uma violação de dados pessoais: Exige que as violações de dados pessoais sejam notificadas às autoridades competentes no prazo de 72 horas.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigos 20–21: Exigem que as entidades essenciais e importantes implementem governação documentada, estratégias de conformidade legal e revisão contínua dos riscos legais.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 5(2) – Quadro de gestão do risco das TIC: Exige a integração da conformidade legal nas funções mais amplas de gestão do risco e supervisão.

11.6.2 Artigo 19 – Risco de terceiros em TIC: Impõe requisitos legais específicos para gerir obrigações contratuais e regulatórias que envolvam fornecedores externos e plataformas.

11.7 COBIT 2019

11.7.1 APO12 – Gerir o risco: Incorpora a conformidade legal e regulatória como componente crítica da governação do risco empresarial.

11.7.2 MEA03 – Monitorizar o cumprimento de requisitos externos: Define a monitorização contínua, o tratamento de exceções e a preparação para auditoria para todas as formas de obrigações regulatórias.