					Insira aqui a designação da entidade jurídica registada							
Número do documento: P33					Título do documento: **Política de Auditoria e Monitorização da Conformidade**							
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 9.2, 9.3, 10	
ISO/IEC 27002:2022	Controlos 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
RGPD da UE	Artigos 24, 32, 33	
Diretiva NIS2 da UE	Artigos 21(2)(g), 27	
DORA da UE	Artigos 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Finalidade

1.1 A finalidade desta política é estabelecer e regular o programa de auditoria e monitorização da conformidade da organização para:

1.1.1 Validar a eficácia dos controlos de segurança e privacidade

1.1.2 Assegurar o alinhamento com as normas aplicáveis, os requisitos legais e as obrigações contratuais

1.1.3 Detetar atempadamente não conformidades, ineficiências e riscos de conformidade

1.1.4 Apoiar a melhoria contínua e a preparação para certificações, avaliações e revisões regulatórias

1.2 Esta política reforça a integridade e a maturidade do Sistema de Gestão da Segurança da Informação (SGSI), através da integração de práticas de auditoria e monitorização estruturadas, orientadas pelo risco e baseadas em evidência.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todas as unidades de negócio, funções e departamentos internos

2.1.2 Instalações físicas, ambientes na cloud, plataformas SaaS e serviços externalizados

2.1.3 Sistemas de informação, aplicações, infraestruturas e ativos de dados abrangidos pelo SGSI

2.1.4 Trabalhadores, prestadores de serviços e prestadores terceiros com obrigações de auditoria ou conformidade

2.2 A política abrange:

2.2.1 Auditorias internas

2.2.2 Auditorias externas/de certificação

2.2.3 Monitorização técnica da conformidade

2.2.4 Auditorias a fornecedores e terceiros

2.2.5 Ações corretivas e preventivas (CAPA)

2.2.6 Métricas, painéis e processos de reporte

2.3 Aplica-se a todos os referenciais relevantes a que a organização está sujeita, incluindo ISO/IEC 27001, RGPD da UE, Diretiva NIS2 da UE, DORA da UE e SOC 2, entre outros.

3. Objetivos

3.1 Verificar a adequação e a eficácia dos controlos, políticas e procedimentos implementados em todo o SGSI e nos ambientes associados.

3.2 Identificar e corrigir quaisquer deficiências, não conformidades ou lacunas de conformidade antes de escalarem para incidentes ou violações.

3.3 Assegurar uma preparação contínua para revisões internas de governação, auditorias externas e certificações independentes.

3.4 Produzir evidência defensável e trilhos de auditoria que suportem solicitações regulatórias, processos judiciais ou pedidos de garantia por parte de clientes ou parceiros.

3.5 Integrar os resultados das auditorias nas atividades mais amplas de gestão do risco, métricas de segurança e melhoria contínua da organização.

4. Papéis e responsabilidades

4.1 Responsável pela Auditoria Interna / Gestor de Conformidade

4.1.1 Planeia, agenda e executa auditorias internas com base na prioridade de risco.

4.1.2 Mantém o Registo de Auditoria, coordena as atividades de auditoria e acompanha as ações corretivas.

4.2 Diretor de Segurança da Informação (CISO)

4.2.1 Assegura que o âmbito da auditoria abrange todos os elementos relevantes do SGSI e os controlos do Anexo A.

4.2.2 Supervisiona a verificação das CAPA e integra os resultados das auditorias no programa de segurança.

[... 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 anualmente pelo Gestor de Conformidade e pelo Diretor de Segurança da Informação, ou mais cedo em resposta a:

9.1.1 Alterações nos referenciais regulatórios, contratuais ou de certificação

9.1.2 Constatações de auditoria significativas ou falhas repetidas de controlos

9.1.3 Reestruturação organizacional ou alterações no sistema GRC

9.1.4 Recomendações de auditores externos ou feedback de reguladores

9.2 O processo de revisão deve avaliar:

9.2.1 A metodologia e a frequência do planeamento de auditorias

9.2.2 Alterações no âmbito do SGSI ou na infraestrutura

9.2.3 Atualizações ao catálogo de controlos ou ao registo legal

9.2.4 A consistência e a qualidade da evidência de auditoria e dos processos CAPA

9.3 Todas as alterações às políticas devem ser:

9.3.1 Documentadas num repositório sujeito a controlo de versões

9.3.2 Aprovadas pela Alta Direção

9.3.3 Comunicadas a todo o pessoal abrangido e integradas em procedimentos atualizados e programas de sensibilização

9.4 A validação pós-revisão deve confirmar que os requisitos atualizados se refletem no Registo de Auditoria, nas ferramentas de conformidade e nos painéis internos de monitorização.

10. Políticas relacionadas e articulações

10.1 Esta política está alinhada com as seguintes políticas organizacionais relacionadas:

10.1.1 P1 – Política de Segurança da Informação: Define o SGSI e estabelece a responsabilização pelo cumprimento e pela melhoria contínua

10.1.2 P5 – Política de Gestão de Alterações: Assegura a visibilidade de auditoria sobre alterações de infraestrutura e configuração que afetem os ambientes de controlo

10.1.3 P6 – Política de Gestão de Riscos: Integra os resultados da auditoria nas atividades de avaliação e tratamento do risco empresarial

10.1.4 P14 – Política de Retenção e Eliminação de Dados: Regula a retenção de evidência de auditoria, logs e registos de conformidade

10.1.5 P18 – Política de Controlos Criptográficos: Suporta o armazenamento e a transferência seguros de dados sensíveis de auditoria

10.1.6 P26 – Política de Segurança de Terceiros e Fornecedores: Abrange direitos de auditoria, documentação de garantia e supervisão da conformidade dos fornecedores

10.1.7 P30 – Política de Resposta a Incidentes: Alinha as auditorias aos processos de tratamento de incidentes com os objetivos de garantia do SGSI

10.1.8 P32 – Política de Continuidade do Negócio e Recuperação de Desastre: Exige a verificação dos testes de continuidade e do cumprimento do plano de recuperação de desastre durante os ciclos de auditoria

11. Normas e referenciais

11.1 Esta política está alinhada com normas globais e requisitos legais para auditoria e validação contínua da conformidade.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 9.2 – Auditoria interna: Exige auditorias regulares e baseadas no risco ao SGSI para avaliar a eficácia e a conformidade.

11.2.2 Cláusula 9.3 – Revisão pela gestão: Os resultados da auditoria devem suportar a revisão estratégica e a melhoria.

11.2.3 Cláusula 10.1 – Não conformidade e ação corretiva: As constatações de auditoria devem ser tratadas através de procedimentos CAPA documentados.

11.3 ISO/IEC 27002:2022 – Controlos 5.35–5.37:

11.3.1 Controlos do Anexo A 5.35–5.37: Abrangem revisão independente, cumprimento de requisitos legais/contratuais e registo para trilho de auditoria.

11.3.2 Fornecem orientações de implementação para planear, executar e melhorar programas de auditoria e conformidade.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Avaliações de controlos: Exige revisão periódica dos controlos de segurança implementados.

11.4.2 CA-5 – Plano de ação e marcos (POA&M): Alinha-se com o acompanhamento e a remediação de constatações de auditoria.

11.4.3 CA-7 – Monitorização contínua: Suporta avaliações de conformidade proativas e automatizadas.

11.5 RGPD da UE (2016/679):

11.5.1 Artigos 24 e 32: Exigem evidência da implementação e eficácia dos controlos de segurança através de estruturas de governação adequadas.

11.5.2 Artigo 33: Sustenta a necessidade de trilhos de auditoria verificados na resposta e notificação de violações.

11.6 Diretiva NIS2 da UE (2022/2555):

11.6.1 Artigo 21(2)(g): Exige a auditoria de políticas e procedimentos como parte das medidas mínimas de gestão do risco de cibersegurança.

11.6.2 Artigo 27: As autoridades nacionais podem realizar ou exigir auditorias a entidades essenciais e importantes.

11.7 DORA da UE (2022/2554):

11.7.1 Artigo 10(2)(e): As entidades devem realizar auditorias internas e externas às práticas de gestão do risco das TIC.

11.7.2 Artigo 25 – Requisitos de auditoria: Exige auditorias periódicas por auditores internos ou auditores externos independentes com visibilidade regulatória.

11.8 COBIT 2019:

11.8.1 MEA01 – Monitorização, Avaliação e Análise do Desempenho e da Conformidade: Assegura que a eficácia dos controlos é verificada e reportada aos órgãos de governação.

11.8.2 MEA03 – Monitorização, Avaliação e Análise da Conformidade: Exige o alinhamento das práticas organizacionais com requisitos legais, contratuais e normativos.