					Insira aqui a designação da entidade jurídica registada							
Número do documento: P33S					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 e 10	Auditorias internas, melhoria contínua e tratamento de não conformidades
ISO/IEC 27002:2022	Controlos 5.35 e 5.37	Revisões internas programadas e revisões independentes de processos externalizados
NIST SP 800-53 Rev.5	CA-2, CA-7 e AU-6	Avaliações de segurança, monitorização contínua e revisão, análise e reporte dos logs de auditoria
RGPD da UE	Artigos 24.º e 32.º	Auditoria das medidas técnicas e organizativas e evidência da eficácia dos controlos
Diretiva NIS2 da UE	Artigo 21.º, n.º 2, alínea f)	Revisão proativa e conformidade suportada por evidência
Regulamento DORA da UE	Artigo 10.º	Gestão do risco das TIC, monitorização e reporte
COBIT 2019	MEA01 e MEA03	Monitorização e avaliação da conformidade e preparação para revisões de terceiros

1. Finalidade

1.1 Esta política estabelece a abordagem da organização à realização de auditorias internas, verificações dos controlos de segurança e monitorização da conformidade regulamentar. Assegura que todos os controlos, políticas, sistemas e prestadores de serviços estão sujeitos a revisão regular e estruturada.

1.2 A finalidade é detetar falhas de controlo, prevenir incumprimentos e demonstrar diligência devida relativamente à ISO/IEC 27001, ao RGPD da UE e a referenciais conexos.

1.3 Permite às PME manter o controlo operacional e a preparação para certificação, mesmo sem uma função de conformidade dedicada, através da utilização de listas de verificação simples e repetíveis e de constatações priorizadas em função do risco.

2. Âmbito

2.1 A presente política aplica-se a:

2.1.1 Todos os departamentos internos e prestadores de serviços externos com responsabilidades relacionadas com sistemas de TI, dados pessoais e serviços críticos para o negócio

2.1.2 Todos os controlos e sistemas abrangidos pelo Sistema de Gestão da Segurança da Informação (SGSI)

2.1.3 Todas as auditorias internas, revisões dos controlos de segurança e verificações de conformidade — quer realizadas internamente, quer por um consultor externo, cliente ou autoridade reguladora

2.2 A presente política também se aplica à recolha de evidência e ao reporte para efeitos de:

2.2.1 Auditorias de certificação e recertificação ISO/IEC 27001

2.2.2 Auditorias de proteção de dados ao abrigo do RGPD da UE ou de obrigações contratuais

2.2.3 Questionários de segurança solicitados por clientes ou avaliações de diligência prévia

2.2.4 Quaisquer revisões regulamentares ou independentes ao abrigo da Diretiva NIS2 da UE ou do Regulamento DORA da UE (quando aplicável)

3. Objetivos

3.1 Assegurar que todos os controlos críticos e as políticas críticas são revistos regularmente quanto à eficácia e à conformidade.

3.2 Manter rastos de auditoria e registos de ações corretivas para demonstrar responsabilização e melhoria contínua.

3.3 Preparar a organização para processos de certificação, recertificação e programas de garantia exigidos por clientes (por exemplo, certificação ISO/IEC 27001 e processos de integração como fornecedor).

3.4 Identificar precocemente lacunas, permitindo a remediação imediata antes de as situações se agravarem ou resultarem em incumprimento de obrigações.

3.5 Permitir ao Diretor-Geral e ao prestador de serviços de TI coordenarem revisões com o mínimo de complexidade, assegurando resultados suportados por evidência e defensáveis.

4. Papéis e responsabilidades

4.1 Diretor-Geral

4.1.1 Supervisiona o programa de auditorias

4.1.2 Aprova os planos de auditoria interna e as constatações

4.1.3 Atribui e acompanha ações corretivas

4.1.4 Autoriza a contratação de auditores externos ou consultores

4.2 Prestador de serviços de TI / Administrador de TI

4.2.1 Fornece evidência durante auditorias internas e externas (por exemplo, logs, configurações e registos de controlo de acesso)

4.2.2 Apoia as verificações técnicas (por exemplo, estado das cópias de segurança e da aplicação de patches)

4.2.3 Mantém o repositório de evidência de auditoria

[... 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 e do plano de auditoria

9.1.1 O Diretor-Geral deve rever esta política e o calendário de auditorias pelo menos uma vez por ano.

9.1.2 A revisão deve avaliar:

9.1.2.1 A eficácia das auditorias na identificação de lacunas

9.1.2.2 A taxa de conclusão das auditorias e das ações corretivas

9.1.2.3 Alterações nos requisitos legais, regulamentares ou de certificação aplicáveis

9.2 Atualizações motivadas por eventos

9.2.1 A política deve ser revista e atualizada quando:

9.2.2 Uma auditoria de certificação ou de acompanhamento resultar numa não conformidade maior

9.2.3 Ocorrerem alterações nos referenciais legais ou regulamentares (por exemplo, novas orientações do RGPD da UE ou transposição nacional da Diretiva NIS2 da UE)

9.2.4 Alterações no negócio afetarem sistemas, processos ou fornecedores incluídos no âmbito da auditoria

9.2.5 Um incidente crítico ou uma violação revelarem lacunas de controlo anteriormente não detetadas

9.3 Documentação das atualizações

9.3.1 Todas as revisões devem ser registadas num registo de versões da política

9.3.2 As atualizações devem ser distribuídas a todos os membros da equipa envolvidos em auditorias

9.3.3 Deve ser incluído um resumo das alterações juntamente com a política atualizada para assegurar a sua compreensão

10. Políticas relacionadas e interligações

10.1 Esta política articula-se com várias outras políticas para PME e reforça-as:

10.1.1 P1S – Política de Segurança da Informação: Estabelece o referencial de base para todas as expectativas de controlo e exige a verificação da sua conformidade através de auditorias.

10.1.2 P2S – Política de Papéis e Responsabilidades de Governação: Estabelece a responsabilização pelo planeamento das auditorias, pela sua execução e pela definição de responsáveis pelas ações corretivas.

10.1.3 P6S – Política de Gestão de Riscos: Identifica deficiências de controlo detetadas em auditorias e assegura que as constatações são documentadas no Registo de Riscos.

10.1.4 P17S – Política de Proteção de Dados e Privacidade: Define os controlos do RGPD da UE que devem ser auditados, incluindo tratamento de dados, resposta a violações e avisos de privacidade.

10.1.5 P22S – Política de Registo em Logs e Monitorização: Fornece os logs de auditoria e os dados forenses utilizados nas revisões de conformidade e de controlos.

10.1.6 P30S – Política de Resposta a Incidentes: Exige a auditoria periódica dos registos de incidentes e das revisões pós-incidente para verificar a eficácia da resposta.

10.1.7 P31S – Política de Recolha de Evidência e Análise Forense: Fornece os procedimentos para recolher, durante auditorias, evidência verificável com cadeia de custódia.

10.2 Em conjunto, estas políticas criam um ciclo fechado de controlo que permite verificação interna, garantia externa e governação alinhada com normas.

11. Normas e referenciais

11.1 ISO/IEC 27001:

11.1.1 Cláusula 9.2 – Exige auditorias internas para avaliar o desempenho do SGSI e o seu alinhamento com os requisitos.

11.1.2 Cláusula 10.1 – Exige melhoria contínua com base nos resultados das auditorias e no tratamento de não conformidades.

11.2 ISO/IEC 27002:

11.2.1 Controlo 5.35 – Exige revisões internas programadas dos controlos e processos.

11.2.2 Controlo 5.37 – Enfatiza revisões independentes, especialmente para processos externalizados.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Avaliações de segurança: exige auditorias aos controlos implementados para verificar a sua eficácia.

11.3.2 CA-7 – Monitorização contínua: enfatiza a deteção proativa e a revisão de deficiências de controlo.

11.3.3 AU-6 – Revisão, análise e reporte dos logs de auditoria: exige a análise regular e o tratamento dos logs de auditoria e das constatações.

11.4 RGPD da UE:

11.4.1 Artigos 24.º e 32.º – Exigem a implementação e a auditoria das medidas técnicas e organizativas, incluindo evidência da eficácia dos controlos e da melhoria ao longo do tempo.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 Artigos 20.º e 21.º – Exigem revisão proativa de controlos, conformidade suportada por evidência e auditabilidade para entidades essenciais e importantes.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitorização, avaliação e análise do desempenho e da conformidade: exige a avaliação periódica do desempenho dos processos e controlos face a normas e objetivos.

11.6.2 MEA03 – Assegurar o cumprimento de requisitos externos: centra-se na monitorização interna e na preparação para auditorias de terceiros e revisões regulamentares.