VISABEIRA
INVESTIGAÇÃO & DESENVOLVIMENTO

Política Geral de Segurança da Informação

ID do Documento	SGSI.PL.01
Versão	5.0
Data da Versão	26 de junho de 2025
Criado por	Comissão de Segurança da Informação e Privacidade
Nível de Classificação	Uso Interno
Aprovado por	Administração

Índice

1 Enquadramento

A **Política de Segurança da Informação** (PSI), constitui um instrumento estratégico da estrutura documental da **Visabeira I&D**, adiante designada por Organização. Esta política orienta a tomada de decisão no domínio da Segurança da Informação, estabelece prioridades claras e sustenta a promoção de uma cultura organizacional orientada para a prevenção e resiliência.

A **Gestão de Topo**, plenamente consciente da importância crítica da Segurança da Informação para a sustentabilidade e competitividade do negócio, assume o compromisso de liderar, promover e assegurar a implementação e melhoria contínua do **Sistema de Gestão da Segurança da Informação (SGSI)**. Neste âmbito, compromete-se a envolver e motivar todos os colaboradores para:

- Reconhecer que a informação, os sistemas, redes, processos de apoio e ativos associados são vitais para a atividade da Organização. A **confidencialidade**, **integridade** e **disponibilidade** da informação são requisitos fundamentais para garantir a eficácia operacional, a rentabilidade, a conformidade e a reputação da Organização no mercado.
- Gerir proativamente os riscos relacionados com a segurança da informação, incluindo os associados ao uso de novas tecnologias (ex: Inteligência Artificial), ao trabalho remoto, e à cadeia de fornecimento, assegurando o cumprimento dos requisitos legais, regulamentares e contratuais aplicáveis.
- Aplicar as melhores práticas, normas e controlos de segurança da informação, sustentando um processo de **melhoria contínua**, orientado por métricas, e capaz de reforçar uma cultura de segurança e de responsabilidade partilhada.
- Assegurar a **continuidade dos processos críticos do negócio**, apoiada por medidas preventivas, planos de continuidade e um SGSI bem estruturado e adaptável à evolução do contexto interno e externo.

Todos os documentos da estrutura organizacional, quer sejam políticas específicas, normas, regulamentos, processos, procedimentos ou modelos de evidência, alinham-se com os princípios e objetivos desta Política, refletindo de forma coerente os compromissos assumidos em matéria de Segurança da Informação.

1.1 Âmbito

A PSI aplica-se a toda a Organização e a todas as entidades sob sua responsabilidade, abrangendo **pessoas, processos, tecnologias e dados** que suportam a atividade organizacional, independentemente do local, formato ou suporte em que a informação se encontre.

Esta política é aplicável a:

- Todos os **colaboradores**, prestadores de serviço, parceiros, fornecedores e quaisquer outras partes externas que tenham acesso à informação ou aos sistemas da Organização;
- Todos os **ativos de informação** da Organização, incluindo dados físicos, digitais e em trânsito, bem como sistemas, redes, aplicações, plataformas digitais, dispositivos inteligentes e equipamentos associados;
- Todos os **processos de negócio**, incluindo os que envolvem desenvolvimento tecnológico, inovação, tratamento de dados e Inteligência Artificial (IA);

- Todos os **ambientes organizacionais**, incluindo instalações físicas, plataformas em nuvem, ambientes on-premises e postos de trabalho remotos.

O âmbito inclui ainda:

- A **adoção e utilização de tecnologias emergentes**, como a Inteligência Artificial e plataformas digitais de apoio ao negócio (ex: sistemas de Tickets - AMIGA Ticket);
- A **gestão da cadeia de fornecimento**, impondo requisitos de segurança da informação a terceiros com base no nível de risco associado;
- A **governança e classificação da informação**, com enfoque na proteção da confidencialidade, integridade e disponibilidade dos dados, e no cumprimento de requisitos legais, regulamentares e contratuais (como o RGPD, AI Act e requisitos fiscais ou de I&D);
- A **continuidade do negócio**, através da gestão de riscos, planos de contingência e recuperação, e preservação da resiliência operacional;

Todas as normas, procedimentos, instruções e modelos operacionais devem estar alinhados com esta política e ser interpretados à luz dos seus princípios e compromissos.

1.2 Finalidade

A PSI define os princípios, objetivos e orientações estratégicas da **Segurança da Informação** na Organização, estabelecendo as bases para uma gestão eficaz e integrada da informação em toda a Organização.

A sua finalidade é:

a) **Estabelecer a estratégia de Segurança da Informação**, alinhada com o modelo organizacional, os objetivos de negócio e os princípios de conformidade e inovação;

b) **Promover uma cultura de segurança**, incentivando comportamentos responsáveis e conscientes por parte de todos os colaboradores, parceiros e prestadores de serviço;

c) **Sensibilizar a comunidade organizacional** para a importância da literacia em segurança da informação, fomentando competências para a identificação, prevenção e resposta a riscos e incidentes;

d) **Integrar a Segurança da Informação como um valor fundamental**, indispensável à continuidade, competitividade e resiliência da Organização;

e) **Avaliar e tratar os riscos de segurança da informação**, através da implementação de controlos adequados, proporcionais ao nível de risco aceitável definido pela Gestão de Topo;

f) **Reforçar a credibilidade, a confiança e a reputação da Organização**, junto dos seus colaboradores, entidades reguladoras, parceiros e demais partes interessadas;

g) **Proteger a informação contra acessos não autorizados, perdas, alterações ou destruição**, resultantes de ações intencionais, negligência, falhas técnicas ou eventos de força maior.

1.3 Revisão e Comunicação

A **PSI** é revista sempre que ocorram alterações relevantes que possam impactar o seu conteúdo, nomeadamente:

- Mudanças no âmbito da Segurança da Informação,
- Alterações na estrutura organizacional,
- Atualização de requisitos legais, regulamentares ou contratuais aplicáveis,
- ou, no mínimo, com uma periodicidade anual.

O objetivo da revisão é assegurar que a PSI se mantém **adequada, eficaz e alinhada** com os objetivos estratégicos da Organização e com o contexto de risco atual.

Após cada revisão, a PSI deve ser **formalmente comunicada a todos os colaboradores** e **disponibilizada às partes interessadas**, sempre que solicitado ou conforme previsto em contratos, auditorias ou obrigações legais.

2 Segurança da Informação

2.1 Definição de Segurança da Informação

A informação e os respetivos repositórios são ativos críticos para a **Visabeira I&D**, essenciais ao funcionamento, inovação e sustentabilidade da Organização. Independentemente do formato, suporte, meio de recolha, transmissão ou armazenamento, a informação deve ser **adequadamente protegida contra ameaças** que possam comprometer a sua confidencialidade, integridade, disponibilidade ou privacidade.

A **Segurança da Informação** consiste na aplicação de um **conjunto de princípios, práticas e controlos**, sustentados por um processo contínuo de **gestão de riscos**, com o objetivo de:

- Proteger os ativos de informação de um leque abrangente de ameaças internas e externas;
- Assegurar a **continuidade das operações da Organização**;
- Maximizar o retorno dos investimentos em tecnologias e processos;
- Assegurar a **conformidade com a norma internacional ISO/IEC 27001** e demais requisitos legais, regulamentares e contratuais aplicáveis.

Com base nesta norma, a Segurança da Informação é formalmente definida como a preservação dos seguintes pilares fundamentais:

Figura 1- Pilares da Segurança da Informação

- **Confidencialidade:** Garantia de que a informação só é acessível a pessoas autorizadas.
- **Integridade:** Salvaguarda da exatidão, consistência e completude da informação.
- **Disponibilidade:** Garantia de acesso à informação e aos ativos correlacionados sempre que necessário por utilizadores autorizados.
- **Privacidade:** Proteção dos dados pessoais e salvaguarda do direito individual à autodeterminação informacional.

2.2 Compromisso Organizacional

A eficácia da Segurança da Informação depende do envolvimento e compromisso de toda a comunidade organizacional. Para tal, devem ser assegurados os seguintes princípios:

- **Sensibilização**: Todos os elementos da Organização devem estar conscientes da importância da segurança da informação e do seu papel na sua manutenção;
- **Responsabilidade partilhada**: A segurança é uma responsabilidade de todos, independentemente da função ou nível hierárquico;
- **Atuação proativa**: A prevenção, deteção e resposta rápida a incidentes devem ser parte da conduta diária;
- **Ética**: O respeito pelos interesses legítimos dos outros deve orientar o uso da informação;
- **Compatibilidade com valores democráticos**: A proteção da informação deve respeitar os direitos, liberdades e garantias fundamentais;
- **Gestão de riscos**: A realização sistemática de análises de risco deve orientar a definição e aplicação de controlos;
- **Segurança por design e por defeito**: A segurança deve ser integrada desde a conceção, desenvolvimento e implementação de infraestruturas, sistemas e processos;
- **Gestão integrada da segurança**: Deve existir uma abordagem coordenada e transversal à gestão da segurança da informação;
- **Gestão de privacidade**: A proteção de dados pessoais deve ser assegurada ao longo de todo o seu ciclo de vida, com base em princípios de minimização e responsabilização;
- **Melhoria contínua**: A política, os controlos e os processos devem ser periodicamente revistos e ajustados em função das necessidades da Organização e do ambiente de risco.

2.3 Compromisso da Gestão de Topo

A **Gestão de Topo** assume o compromisso de liderar, apoiar e promover ativamente a Segurança da Informação como um elemento estratégico para a sustentabilidade, competitividade e inovação da Organização.

Para garantir o cumprimento dos objetivos definidos no SGSI, compromete-se a:

- **Cumprir todos os requisitos legais, regulamentares, normativos e contratuais aplicáveis**, incluindo os relativos à proteção de dados pessoais, à gestão de riscos tecnológicos, à utilização ética da Inteligência Artificial, à cibersegurança e à conformidade com a norma ISO/IEC 27001;
- **Assegurar o alinhamento entre a governação da informação, a operação dos sistemas e o modelo organizacional**, promovendo uma abordagem integrada que envolva todas as áreas da Organização;
- **Estabelecer, implementar, manter e melhorar continuamente o SGSI**, com base numa gestão de risco dinâmica, assegurando a eficácia dos controlos e a capacidade de adaptação a novos desafios, ameaças e oportunidades (tecnológicas, organizacionais ou legais);
- **Promover a cultura de segurança e responsabilidade partilhada**, envolvendo colaboradores, parceiros, fornecedores e todas as partes interessadas;
- **Incorporar a segurança da informação nos processos de inovação, digitalização e adoção de tecnologias emergentes**, garantindo que novos sistemas (como plataformas digitais, sensores inteligentes ou soluções baseadas em IA) integram requisitos de segurança desde a fase de conceção;
- **Integrar a segurança da informação com políticas e objetivos transversais**, como a sustentabilidade, a ética digital, o ESG e a proteção dos direitos fundamentais dos titulares de dados.

2.4 Objetivos de Segurança da Informação

Com vista à melhoria contínua do seu desempenho e da eficácia do SGSI, a Organização definiu **Objetivos Estratégicos** de Segurança da Informação, alinhados com os seus valores, políticas internas, metas de inovação e responsabilidade organizacional.

Estes objetivos visam proteger os ativos de informação, garantir a continuidade do negócio, assegurar a conformidade legal e regulamentar, e fomentar uma cultura organizacional de segurança e confiança.

Os Objetivos de Segurança da Informação da Organização são:

- **Avaliar, tratar e monitorizar os riscos de segurança da informação**, com base em metodologias consistentes de gestão de risco, de forma a implementar controlos eficazes e garantir que os riscos residuais se mantêm dentro do nível de aceitação definido pela Organização;
- **Promover uma cultura de segurança sólida e transversal**, através de ações regulares de **formação, sensibilização e capacitação**, adaptadas aos diferentes perfis funcionais, incluindo tópicos como literacia digital, proteção de dados, uso responsável de IA e prevenção de incidentes;

- **Gerir de forma segura e auditável os acessos e perfis de utilizador**, assegurando que as permissões atribuídas são compatíveis com as responsabilidades, as competências e o princípio do menor privilégio;
- **Definir e aplicar controlos técnicos e organizacionais adequados** para garantir a **confidencialidade, integridade, disponibilidade, rastreabilidade, auditabilidade e privacidade** da informação ao longo de todo o seu ciclo de vida;
- **Integrar a segurança da informação desde a fase de conceção ("security and privacy by design")** em todos os projetos de desenvolvimento tecnológico, transformação digital e adoção de novas soluções;
- **Adotar uma abordagem de melhoria contínua**, com base em indicadores, auditorias, revisões e lições aprendidas, de forma a evoluir para níveis de maturidade superiores no SGSI e responder com agilidade às mudanças no contexto tecnológico, regulatório e de ameaças.

3 Implementação da Política de Segurança da Informação

3.1 Contexto

- A informação, assim como todos os seus processos de apoio, sistemas, redes e ativos digitais, são recursos estratégicos e essenciais para o negócio da Organização. A **confidencialidade, integridade, disponibilidade e privacidade da informação** são pilares fundamentais para garantir a competitividade, receita, rentabilidade e reputação da Organização no mercado.
- No contexto atual, a segurança dos sistemas de informação enfrenta desafios crescentes devido à diversidade e sofisticação das ameaças, incluindo **fraudes eletrónicas, ciberataques avançados, espionagem corporativa, fugas de dados, sabotagem, ataques de negação de serviço (DoS) e ameaças internas**, que evoluem constantemente em escala e complexidade.
- A crescente dependência de sistemas e serviços digitais, aliada ao uso disseminado de redes públicas e privadas e à partilha intensiva de recursos de informação, aumenta a complexidade da gestão dos acessos e da proteção dos dados, tornando a Organização mais vulnerável a incidentes de segurança.
- A identificação dos requisitos de segurança da informação é realizada por meio de **análises de risco estruturadas**, que avaliam a exposição a ameaças e vulnerabilidades, possibilitando a priorização dos riscos mais relevantes e a definição de medidas de mitigação eficazes, alinhadas com as melhores práticas e normas internacionais.
- A PSI constitui o **referencial fundamental e orientador para a elaboração, implementação e revisão de todos os documentos, processos e decisões operacionais e táticas relacionados à Segurança da Informação**. Esta política é sustentada por um conjunto integrado de **Políticas, Normas, Procedimentos, Instruções de Trabalho e Regras**, que garantem a coerência e efetividade do Sistema de Gestão de Segurança da Informação.
- Além disso, a PSI incorpora a necessidade de alinhamento com as diretrizes de **proteção de dados pessoais e privacidade**, princípios éticos e de responsabilidade digital, e apoia as iniciativas de sustentabilidade e

governança ambiental, social e corporativa da Organização, promovendo uma abordagem integrada e sustentável à segurança da informação.

3.2 Incumprimento

Qualquer ação que viole a PSI, bem como as demais políticas, normas, procedimentos, regras ou instruções de trabalho relacionadas com o SGSI, que comprometa os controlos de segurança implementados, estará sujeita a sanções civis, penais e administrativas, de acordo com a legislação vigente e regulamentos aplicáveis, podendo estas ser aplicadas isolada ou cumulativamente.

As penalidades serão aplicadas de forma proporcional à gravidade da infração, seguindo os procedimentos disciplinares internos da Organização, que asseguram transparência e justiça no tratamento dos casos. Dependendo da natureza e impacto da contraordenação, as ações disciplinares poderão incluir advertências, suspensão temporária de acesso, suspensão ou até a cessação da relação contratual ou laboral com a Organização.

Em todos os casos, aplica-se o previsto no Código Penal e no Código Civil, bem como as normas, regulamentos, processos e procedimentos internos da Organização.

3.3 Tratamento de exceções

Os objetivos de Segurança da Informação são mais facilmente alcançados quando os requisitos, processos e procedimentos são uniformes e aplicados a todas as unidades funcionais, funções e serviços da Organização.

No entanto, reconhece-se que determinadas normas, processos ou procedimentos podem não ser viáveis ou adequados para unidades específicas, projetos em curso, novos equipamentos ou aplicações recentemente implementadas. É expectável que, no âmbito das atividades da Organização, surjam situações ou cenários excecionais que não possam ser eficazmente geridos estritamente dentro dos requisitos estabelecidos na PSI ou na documentação correlacionada.

Embora o desvio dos processos e procedimentos padrão seja desencorajado, situações excecionais podem justificar a adoção de alternativas, desde que estas estejam devidamente fundamentadas por uma justificação consistente, alinhada com os princípios da Segurança da Informação, e disponham dos recursos necessários para garantir a implementação e manutenção adequadas desses requisitos alternativos.

4 Organização da Segurança da Informação

4.1 Informação Documentada

Com objetivo de satisfazer os requisitos do referencial normativo ISO/IEC 27001, a Organização elaborou um conjunto de políticas e procedimentos específicos e os seus principais controlos.

A criação, manutenção, análise crítica, melhoria e distribuição de todos os documentos do SGSI são da responsabilidade da Comissão de Segurança e Privacidade que realiza a consulta a outras áreas relevantes sempre que necessário.

4.1.1 Estrutura Documental

Para assegurar a gestão efetiva de Segurança da Informação existe e é mantida uma estrutura documental responsável pela orientação, planeamento, implementação, manutenção e melhoria das práticas de Segurança da Informação.

Esta estrutura abrange vários níveis para descentralizar as responsabilidades da gestão da Segurança da Informação pelas várias áreas da Organização. Os níveis em relação aos quais o SGSI estabelecido pela Organização está documentado e mantido são:

- **Nível 1** Orientações gerais e compromissos da Organização no seu contexto interno e a sua relação com o contexto externo.
- **Nível 2** Documentos base que constituem e explicam o funcionamento do SGSI, dando assim suporte para todos os outros documentos provenientes da segurança da informação, tendo em conta as exigências das normas de referência, requisitos legais aplicáveis e metodologias de trabalho aplicáveis.
- **Nível 3.1** Políticas que divulgam as diretrizes, os controlos, os deveres e especificações para as várias áreas de segurança da informação.
- **Nível 3.2** Os procedimentos constituem um meio de clarificar pormenores e aspetos específicos de atividades ou tarefas de uma determinada política. As instruções de trabalho são documentos com descrições detalhadas de "como se faz", documentos para consulta quando é necessário realizar uma determinada tarefa, atividade ou serviço.
- **Nível 3.3** Os registos são resultado do preenchimento de algum modelo de impresso. Através dos registos é possível dispor de elementos de avaliação do desempenho do SGSI, sendo que estes suportam ou criam evidências da conformidade das ações efetuadas.

A estrutura documental da Segurança da Informação está definida na *Framework* de Documentação de Segurança da Informação da Organização.

4.2 Responsabilidades

A Organização estabelece de forma clara as funções, responsabilidades e autoridades de todos os colaboradores através dos seguintes documentos estruturantes:

- **Manual de Funções**
- **Processos**
- **Políticas e Procedimentos de Segurança da Informação**
- **Documentação Operacional**, como Instruções de Trabalho, Registos e outros documentos de apoio

As responsabilidades específicas no âmbito do SGSI devem ser consultadas nos documentos relevantes que o compõem. No entanto, independentemente da função ou nível hierárquico, todos os utilizadores, incluindo a Gestão de Topo e os membros da estrutura organizacional de Segurança da Informação, têm o dever de adotar comportamentos responsáveis e alinhados com os princípios e objetivos da Segurança da Informação.

Neste sentido, cada colaborador da Organização deve:

- **Conhecer, respeitar e aplicar** as regras e responsabilidades definidas na presente Política, bem como nas normas e procedimentos internos, especialmente no que respeita à utilização dos recursos de Tecnologias de Informação e Comunicação (TIC).
- **Cumprir o código de conduta** e observar todos os requisitos legais aplicáveis à sua função, com particular atenção à legislação sobre proteção de dados e confidencialidade.
- **Assumir responsabilidade pelas suas ações**, incluindo violações às regras de utilização dos sistemas e recursos de informação, sujeitando-se às penalidades previstas nos regulamentos internos e na legislação aplicável.
- **Comunicar, de imediato**, qualquer falha, incidente ou não conformidade relacionada com a Segurança da Informação, conforme estabelecido no Procedimento de Gestão de Incidentes.
- **Abster-se de ocultar a sua identidade** ou assumir a identidade de outrem na utilização de sistemas ou recursos de informação da Organização.
- **Proteger os seus meios de autenticação**, como palavras-passe, cartões, tokens ou outros dispositivos de segurança, assegurando a sua confidencialidade e nunca os partilhando com terceiros.
- **Assumir total responsabilidade pelo uso da sua conta de utilizador**, inclusive por ações indevidas realizadas sob as suas credenciais.
- **Divulgar informação confidencial e interna** apenas nos termos legalmente previstos, recorrendo sempre que necessário a aconselhamento jurídico ou deontológico antes de o fazer.
- **Adotar boas práticas na utilização de equipamentos e no tratamento da informação**, contribuindo ativamente para a robustez e eficácia do SGSI.

4.3 Avaliação de Desempenho

4.3.1 Indicadores de Desempenho (KPI)

Os KPI são instrumentos fundamentais para avaliar o desempenho da Segurança da Informação e a eficácia dos controlos implementados no âmbito do SGSI.

A definição dos KPI segue a metodologia **SMART** - *Specific, Measurable, Achievable, Relevant e Time-bound* - e obedece aos seguintes princípios orientadores:

- **Alinhamento estratégico** com a PSI e com os objetivos definidos para a Segurança da Informação.
- **Mensurabilidade e fiabilidade**, permitindo a recolha de dados consistentes, objetivos e verificáveis ao longo do tempo.
- **Comparabilidade e reprodutibilidade**, garantindo a obtenção de resultados que possam ser analisados de forma consistente entre diferentes períodos ou contextos.
- **Relevância e utilidade prática**, assegurando que os indicadores selecionados contribuem efetivamente para a monitorização e melhoria contínua do SGSI.

Os KPI são monitorizados e medidos com periodicidade definida, sendo **revistos anualmente no âmbito da Revisão pela Gestão**, com o objetivo de validar a sua

atualidade, relevância e capacidade de suportar a tomada de decisão sobre o desempenho e a eficácia do SGSI.

4.3.2 Auditoria Interna

As auditorias internas ao SGSI são **planeadas e executadas anualmente** pela **Comissão de Segurança da Informação e Privacidade (CSIP)**, com o objetivo de avaliar sistematicamente a **eficácia, eficiência e conformidade** das políticas, procedimentos e controlos implementados, bem como de promover a **melhoria contínua do SGSI**.

No âmbito do plano anual de auditoria, é realizada pelo menos uma auditoria interna que inclui as seguintes áreas:

- **Proteção de Dados**, com base no Regulamento Geral sobre a Proteção de Dados (RGPD) e nos normativos internos aplicáveis.
- **Segurança da Informação**, com base nos requisitos da norma ISO/IEC 27001, complementada pelas boas práticas reconhecidas no setor.

As auditorias são conduzidas por pessoal qualificado, com independência face às atividades auditadas, e os seus **resultados são documentados em relatórios de auditoria**, contendo eventuais não conformidades, oportunidades de melhoria e ações corretivas ou preventivas recomendadas.

Estes relatórios são **apresentados à Gestão de Topo, à Gestão de Negócio e à Equipa de Segurança da Informação** da Organização, assegurando o envolvimento das partes interessadas e a devida responsabilização no seguimento das conclusões da auditoria.

4.3.3 Revisão pela Gestão

O SGSI implementado pela Organização é revisto, pelo menos uma vez por ano, pela Comissão de Segurança de Informação e Privacidade de modo a garantir a sua contínua aplicabilidade, adequabilidade e eficácia. Esta revisão é baseada nos requisitos da norma ISO/IEC 27001, bem como as orientações complementares aplicáveis.

As conclusões da Revisão pela Gestão são **documentadas numa ata formal**, incluindo as decisões e ações a adotar para **melhorar continuamente o SGSI**, abordar necessidades de mudança, otimizar recursos e assegurar o cumprimento sustentado dos objetivos de segurança da informação.

5 Segurança da Informação para Fornecedores

Com o objetivo de proteger os ativos de informação da Organização e assegurar a continuidade e a resiliência das operações, foi estabelecido um **processo estruturado e controlado para a seleção, contratação, monitorização e revisão de fornecedores e prestadores de serviços**, conforme definido na documentação do SGSI.

Este processo está alinhado com os princípios de **gestão de riscos da cadeia de fornecimento**, com foco na proteção da confidencialidade, integridade,

disponibilidade e rastreabilidade da informação partilhada ou acessível por entidades externas.

5.1 Generalidades

Os requisitos de segurança aplicáveis aos fornecedores incluem:

- **Clareza de responsabilidades**: Todas as entidades externas que prestem serviços à Organização devem compreender e aceitar as suas responsabilidades e funções, de forma a mitigar o risco de roubo, fraude, acesso indevido ou uso abusivo da informação e das infraestruturas de processamento de dados.
- **Cláusulas contratuais obrigatórias**: Todos os contratos com fornecedores devem incluir cláusulas específicas de **confidencialidade**, **proteção de dados**, **segurança da informação** e **conformidade legal**, garantindo que os terceiros se comprometem a salvaguardar toda a informação a que tenham acesso, seja de natureza técnica, organizacional ou financeira.
- **Acordos de confidencialidade**: Sempre que aplicável, as entidades externas que acedam ou utilizem infraestruturas, sistemas ou dados da Organização devem **assinar acordos complementares de confidencialidade**, definindo os seus deveres em matéria de proteção da informação, sobretudo quando tais aspetos não estiverem suficientemente detalhados nos contratos.
- **Avaliação de risco**: A seleção e manutenção de fornecedores considera uma **avaliação de riscos de segurança da informação**, proporcional ao impacto e criticidade dos serviços prestados, conforme metodologia definida no SGSI.

5.2 Monitorização e Avaliação de Desempenho

Os serviços prestados por fornecedores são objeto de **monitorização sistemática** com base em critérios previamente definidos e alinhados com os objetivos de segurança da informação.

A avaliação contínua permite garantir que os fornecedores mantêm níveis adequados de conformidade e desempenho, bem como a evolução dos seus controlos de segurança.

5.3 Alteração nos Serviços

As alterações à provisão dos serviços, incluindo manter e melhorar as políticas de segurança da informação, os procedimentos e os controlos existentes, devem ser geridas tendo em atenção a criticidade dos sistemas e baseada na reavaliação dos riscos. A Organização irá controlar como são desenvolvidas e implementadas as alterações dos serviços prestados pelos fornecedores.

6 Ciclo PDCA do Sistema de Gestão de Segurança da Informação

O **ciclo PDCA (Plan–Do–Check–Act)** é a metodologia adotada pela Organização para estruturar, implementar e melhorar continuamente o SGSI. Este ciclo assegura que os processos são planeados de forma estratégica, executados com os recursos

adequados, monitorizados com indicadores relevantes e revistos de forma sistemática, promovendo decisões baseadas em evidências.

O PDCA permite, assim, identificar oportunidades de melhoria e assegurar a **eficácia, adequabilidade e alinhamento do SGSI com os objetivos organizacionais e requisitos legais e normativos**.

Esta metodologia pode ser observada na Figura seguinte.

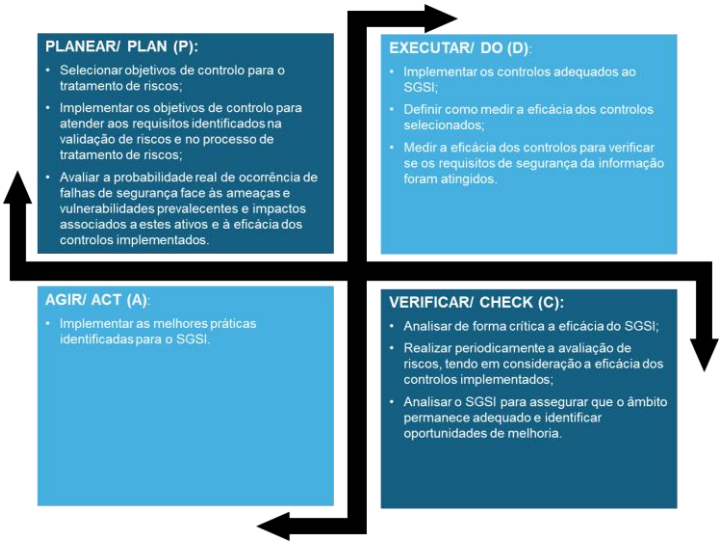

Figura 2- Ciclo PDCA do Sistema de Gestão da Segurança da Informação

6.1 Melhoria Contínua

A Organização compromete-se com a **melhoria contínua do SGSI**, assegurando que este se mantém eficaz, atualizado e adaptado ao contexto interno e externo. Para isso:

- São realizadas **revisões periódicas**, previamente planeadas ou desencadeadas por **alterações significativas**;
- São consideradas as **não conformidades**, os **resultados de auditorias**, as **ações corretivas**, as **lições aprendidas** e os **indicadores de desempenho (KPI)** como base para a tomada de decisão;
- As ações de melhoria podem incluir a **atualização de políticas e procedimentos**, o **reforço de controlos**, a **formação adicional para colaboradores** ou a **reformulação de processos**.

7 Referências

Este documento foi criado com base nas melhores práticas e standards do mercado, nomeadamente:

- Norma ISO/IEC 27001.