



Política de Gestão da Segurança da Informação

V3.0

**CLASSIFICAÇÃO DO DOCUMENTO
USO PÚBLICO**

Este documento quando impresso constitui uma
cópia não controlada

Índice

1. OBJETIVO DA POLÍTICA.....	3
2. ÂMBITO DE PROTEÇÃO PARA A SEGURANÇA DA INFORMAÇÃO	3
3. COMPROMISSOS PARA A SEGURANÇA DA INFORMAÇÃO	3
4. SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI).....	4
5. GESTÃO DO RISCO.....	4
6. INTEGRAÇÃO COM A GESTÃO DA PRIVACIDADE DE DADOS PESSOAIS	4
7. CIBERSEGURANÇA.....	4
8. REVISÃO E ATUALIZAÇÃO	5
9. DIVULGAÇÃO	5

1. OBJETIVO DA POLÍTICA

A informação é considerada pela ActiveSys como um ativo estratégico, fundamental e de considerável valor para a operacionalidade dos seus processos de negócio.

A gestão de topo da ActiveSys entende como fundamental a definição e aplicação de uma política que defina os seus compromissos para a proteção dessa informação, tendo identificado um seu representante que assume o papel de Liderança para a gestão da segurança da informação.

A Liderança será responsável pela garantia de que esta política se mantém adequada para os objetivos da organização e que esteja em condições de sustentar a definição e operacionalização de um Sistema de Gestão de Segurança de Informação (doravante denominado por "SGSI").

A Liderança do SGSI compromete-se a disponibilizar os necessários recursos e suporte, bem como levará a cabo a missão de garantir a melhoria contínua de tais compromissos e respetivas métricas de eficácia, por forma a assegurar a execução dos requisitos e expectativas das partes interessadas identificados para o SGSI.

2. ÂMBITO DE PROTEÇÃO PARA A SEGURANÇA DA INFORMAÇÃO

O âmbito de proteção onde se aplica esta política está descrito pelo documento ASYS-SEG-007-ASGSI, onde se pode encontrar a sua definição como sendo:

"O âmbito de Proteção do Sistema de Gestão da Segurança da Informação da ActiveSys inclui a protecção da CID – Confidencialidade, Integridade e Disponibilidade das atividades referentes aos seus processos comercial, pré-venda, compras e gestão de recursos humanos, independentemente do local onde se executam as mesmas."

3. COMPROMISSOS PARA A SEGURANÇA DA INFORMAÇÃO

A presente Política define os compromissos assumidos pela ActiveSys para a segurança da informação no âmbito de proteção, que consistem nas seguintes garantias:

- **Confidencialidade** – Assegurar que apenas os colaboradores formalmente autorizados têm acesso à informação classificada como confidencial pela Liderança do SGSI
- **Integridade** – Assegurar a proteção da informação contra a modificação e/ou destruição não autorizada, salvaguardando a respetiva veracidade e autenticidade
- **Disponibilidade** – Assegurar que o acesso à informação é realizado sempre que necessário para a realização de uma atividade, preservando a confidencialidade, privacidade e integridade

Em complemento, a Liderança do SGSI entende que se devem adicionar os seguintes compromissos complementares, mas devidamente integrados:

- **Privacidade** – Assegurar que os dados pessoais dos respetivos titulares, classificados como informação confidencial, apenas são recolhidos, processados e armazenados de acordo com as respetivas autorizações concedidas pelo titular.
- **Autenticidade** – Assegurar que os colaboradores da ActiveSys utilizam métodos e práticas robustas para a sua autenticação nos sistemas aplicativos e recursos que utilizam para o desenvolvimento das suas atividades no âmbito de protecção.
- **Não Repúdio** – Assegurar que todos os colaboradores da ActiveSys, quando na condição de emissores de informação ou quando partilham dados pessoais com destinatários autorizados, serão sempre identificados física e digitalmente com valor probatório legal.

4. SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

O SGSI da ActiveSys tem como missão a definição, implementação, manutenção e melhoria contínua de um conjunto de regras, práticas, controlos de segurança, ações de monitorização e auditoria que permitam garantir a execução dos compromissos assumidos pela organização e seus colaboradores no âmbito de proteção para a Segurança da Informação.

Para atingir com eficácia os compromissos e objetivos assumidos na presente política serão adotados os seguintes mecanismos de operacionalização:

- Definição, aprovação e divulgação de políticas temáticas complementares para a gestão da Segurança da Informação;
- Promoção de ações de sensibilização, formação e treino dos colaboradores internos e externos;
- Análise e gestão dos riscos identificados, incluindo o(s) respetivo(s) plano(s) de tratamento do risco e o respetivo risco residual;
- Identificação e operacionalização de controlos de segurança para tratamento do risco;
- Gestão dos incidentes de segurança de informação e respetivas respostas para garantia da continuidade de negócio nas atividades definidas no âmbito de proteção;
- Realização de auditorias internas para identificação de oportunidades de melhoria;
- Revisão do sistema de gestão e respetivas métricas de eficácia.

5. GESTÃO DO RISCO

Por se considerar uma ferramenta imprescindível no cumprimento dos objetivos do SGSI, serão feitas periodicamente análises de risco para que sejam adotadas as medidas de tratamento adequadas e proporcionais aos níveis do risco identificados.

Os controlos de segurança a implementar serão selecionados em função dos resultados dessa análise, com objetivo de assegurar a redução do risco com eficácia e a minimização do risco residual.

6. INTEGRAÇÃO COM A GESTÃO DA PRIVACIDADE DE DADOS PESSOAIS

Através da definição da garantia de privacidade como um dos compromissos da segurança da informação, a ActiveSys executa a implementação integrada de controlos de segurança que assegura as medidas de tratamento do risco adequadas para cumprimento dos requisitos do Regulamento Geral de Proteção de Dados e na estrita conformidade para com a de Política RGPD.

7. CIBERSEGURANÇA

A informação e dados pessoais utilizados pelos processos da organização no âmbito de proteção serão protegidos adequadamente contra os ataques e ameaças externos ou internos que sejam realizados através de mecanismos ou métodos que coloquem em causa a Cibersegurança da organização e dos seus colaboradores.

Para o efeito, serão adotadas todas as boas práticas recomendadas pela European Union Agency for Cybersecurity (ENISA), pela National Institute of Standards and Technology (NIST) e pelo CNCS (Centro Nacional de Cibersegurança) que permitam implementar controlos de segurança e procedimentos necessários para identificar e tratar tais ataques ou ameaças, assim como medidas de prevenção e proteção adequadas e proporcionais para assegurar o cumprimento das obrigações assumidas na presente política.

Em complemento, a ActiveSys compromete-se a assegurar conformidade para com o QNRCS – Quadro Nacional de Referência de Cibersegurança e para com o RJSC – Regulamento Jurídico de Segurança no Ciberespaço.

8. REVISÃO E ATUALIZAÇÃO

O presente documento será revisto e atualizado sempre que existirem alterações de contexto e estratégia da empresa, alterações da lista de partes interessadas e respectivos requisitos, ou ainda devido à realização de alterações organizativas relevantes nos seus processos de negócio.

A Liderança do SGSI compromete-se ainda que esta revisão e atualização será realizada pelo menos anualmente.

9. DIVULGAÇÃO

A classificação deste documento permite a sua consultada pelo publico em geral.