

Política de Segurança da Informação ABAI

Este documento é propriedade da ABAI e destina-se apenas ao uso interno. São proibidas a sua reprodução total ou parcial, distribuição, comunicação pública e transformação.

Preparado por	Revisto por	Aprovado por
ABAI Group (CISO / Comité de Segurança)	Direção de IT	Comité de Segurança ABAI Group
Data: 09/02/2023	14/04/2023	24-05-2023

Registo de Modificações			
Versão	Data	Descrição da alteração	Autor da modificação
1.0	24/05/2023	Primeira Versão	Não Aplicável

Este documento é propriedade da ABAI e destina-se apenas ao uso interno. São proibidas a sua reprodução total ou parcial, distribuição, comunicação pública e transformação.

ÍNDICE

OBJECTIVO DA POLÍTICA	4
ÂMBITO	4
RESPONSABILIDADES	4
QUADRO LEGAL	5
CLASSIFICAÇÃO DA INFORMAÇÃO	5
IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA	5
FORMAÇÃO E SENSIBILIZAÇÃO	5
AUDITORIA	6
PLANOS ESPECÍFICOS	6

OBJETIVO DA POLÍTICA

O Comité de Gestão da ABAI reconhece que a informação e os sistemas que a suportam são bens estratégicos, e por isso está determinado a atingir os níveis de segurança necessários para garantir a sua proteção.

O objetivo da Política de Segurança da Informação é fornecer diretrizes para garantir a segurança da informação e melhorar a qualidade dos serviços que a ABAI oferece aos seus clientes.

ÂMBITO

Esta política abrange toda a informação utilizada pela ABAI para o desenvolvimento das suas atividades e é aplicável, numa base obrigatória, a todos os colaboradores da ABAI, bem como às entidades parceiras envolvidas na utilização da informação e dos sistemas.

As relações com estas entidades parceiras devem ser sempre cobertas pelos contratos de prestação de serviços correspondentes, incluindo cláusulas que garantam a salvaguarda na utilização da informação.

A política de segurança aplica-se a todas as fases do ciclo de vida dos dados: geração, distribuição, armazenamento, processamento, transporte, consulta e destruição; e dos sistemas que os processam: análise, conceção, desenvolvimento, implementação, operação e manutenção.

Esta política prossegue a adoção de ações destinadas a preservar as quatro componentes básicas da segurança da informação:

- **Confidencialidade:** Assegurar que apenas pessoas devidamente autorizadas tenham acesso aos dados e sistemas.
- **Integridade:** Assegurar a precisão da informação e dos sistemas contra alterações acidentais ou fraudulentas, perda ou destruição.
- **Disponibilidade:** Assegurar que a informação e os sistemas podem ser utilizados como e quando necessário.
- **Rastreabilidade:** Assegurar que qualquer ação ou transação possa ser rastreada de forma única, assegurando a conformidade com os controlos estabelecidos nas políticas, procedimentos e regulamentos relevantes.

RESPONSABILIDADES

A função de segurança reside no Comité de Segurança Corporativo. Com dependência funcional e autoridade delegada, o gestor da segurança da informação e o gestor da segurança física canalizam as orientações e regulamentos da ABAI.

O Comité de Segurança Corporativa estabelece e supervisiona os Sub-Comités de Segurança em cada país onde a ABAI opera, e os Sub-Comités Corporativos que considera necessários,

nos quais delega a gestão da segurança de questões específicas.

As organizações utilizadoras e de apoio, em conformidade com os regulamentos de segurança, devem implementar os controlos necessários com a assistência da organização de segurança corporativa e local do país.

O departamento tecnológico é responsável pela segurança das plataformas, redes e infraestruturas de processamento de informação, prestando serviço aos outros departamentos ABAI que possuem e/ou armazenam informação, de acordo com as necessidades de segurança que exigem, de acordo com os regulamentos estabelecidos e os requisitos dos clientes.

Cada utilizador dos sistemas é responsável pela correta utilização dos sistemas e pelo cumprimento das obrigações e controlos estabelecidos.

QUADRO LEGAL

A ABAI está empenhada em assegurar o cumprimento da legislação em vigor sobre a proteção e segurança da informação e sistemas aplicáveis a todos os seus processos corporativos, nos países em que opera.

CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações devem ser classificadas em virtude da sua importância para a organização e tratadas de acordo com essa classificação, em conformidade com as disposições dos regulamentos sobre classificação e tratamento de informações.

IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

Para poder aplicar as linhas de ação definidas nesta política, é necessário definir, elaborar, implementar e manter planos de segurança e continuidade, tanto a nível corporativo como em cada empresa do Grupo, onde estão incluídos:

- O conjunto de regulamentos, normas, diretrizes e procedimentos operacionais que determinam a forma adequada de agir em matéria de segurança.
- Projetos de investimento que proporcionem os meios necessários para alcançar estes objetivos.
- Organizações responsáveis pela gestão da segurança nos seus vários aspetos.
- Os métodos de controlo, revisão e ajustamento para verificar o correto funcionamento dos planos de segurança e continuidade.

O desenvolvimento de planos de segurança e continuidade deve ser acompanhado por análises formais de risco e processos de gestão de risco para permitir a implementação de soluções adequadas, ou para assumir os riscos associados a desvios destas soluções.

FORMAÇÃO E SENSIBILIZAÇÃO

O método mais eficaz para melhorar a segurança é através da formação contínua e da sua incorporação no local de trabalho.

Os planos de formação incluirão cursos específicos sobre segurança da informação de acordo com a área alvo: gestão, técnicos, administradores e utilizadores do sistema. Do mesmo modo, serão realizadas campanhas de sensibilização sobre segurança para todo o pessoal da ABAI, fornecedores e clientes, por qualquer meio considerado mais eficaz.

AUDITORIA

Os sistemas de informação serão periodicamente sujeitos a auditorias internas ou externas, a fim de verificar o correto funcionamento dos planos de segurança, determinar os graus de conformidade e recomendar medidas corretivas.

PLANOS ESPECÍFICOS

Qualquer plano de segurança específico deve estar de acordo com as disposições e recomendações mais gerais e abrangentes deste documento.

EFETIVIDADE

A Política de Segurança da Informação Empresarial entra em vigor no dia da sua publicação.