Rev.	Data da aprovação	Descrição da revisão
01.2	14/10/2025	Alterada a referência da norma NBR ISO27701 para versão 2026, incluída a Lei nº 13.709/2018 – LGPD e revisado todo o documento.
01.1	16/09/2025	Retirado o termo 'empregados', pois já consta 'colaboradores', no item 2. Acrescentadas referências a 'Privacidade'. Retirados fornecedores no item 6.8. Incluído "testes de segurança e aceitação" no item 6.11. Incluído "autenticação segura" no item 6.13
01	28/08/2024	Alteração do nome da empresa e do e-mail de contato com SI e Privacidade. Inclusão de referência à "Política de SI para Fornecedores" no item 6.4, Inclusão de Sumário, inclusão da Política Externa de Privacidade no item 3.
00	13/06/2023	Criação do documento.

Elaborado por:	Analisado por:	Aprovado por:
Aline Giuliani e Maria Eduarda (Consultoria)	Equipe GRC (Governança, Riscos e Compliance) de SI e Privacidade	Gerência de GRC (Governança, Riscos e Compliance) de SI e Privacidade

Cópia Controlada

Reprodução Proibida

SUMÁRIO

1. Objetivo 3
2. Campo de aplicação 3
3. Referências 4
4. Definições 4
5. Responsabilidades 5
6. Diretrizes 6
   - 6.1. Diretrizes gerais 6
   - 6.2. Regulamentação 7
   - 6.3. Riscos e ameaças 7
   - 6.4. Fornecedores 7
   - 6.5. Auditorias 8
   - 6.6. Continuidade de negócios 8
   - 6.7. Classificação da informação 8
   - 6.8. Treinamento e conscientização 8
   - 6.9. Tratamento de incidentes 8
   - 6.10. Segurança da informação e privacidade no gerenciamento de projetos 9
   - 6.11. Desenvolvimento seguro de sistemas 10
   - 6.12. Segurança nas comunicações 10
   - 6.13. Cópias de segurança 11
   - 6.14. Proteção e privacidade de dados pessoais 11
   - 6.15. Análise crítica de segurança da informação 11
   - 6.16. Melhoria contínua 11
7. Disposições finais 11
8. Anexos 12

Cópia Controlada

Reprodução Proibida

1. OBJETIVO

Estabelecer diretrizes para garantir a segurança das informações corporativas, buscando o equilíbrio entre performance e confiabilidade, objetivando a perenidade dos negócios da AlmavivA Experience, fundamentadas nos seguintes itens:

- Alinhamento dos objetivos estratégicos de Segurança da Informação e Privacidade com os objetivos de negócio das empresas;
- Redução dos impactos decorrentes de eventos de Segurança da Informação.
- Identificação dos principais riscos de segurança da informação e privacidade aplicáveis ao negócio.
- Disseminação das normas e diretrizes de segurança da informação e privacidade a todos os profissionais da AlmavivA Experience, terceiros aplicáveis e qualquer pessoa relacionada a expansão dos negócios da AlmavivA Experience.

A Alta Liderança e o Comitê de Segurança da Informação e Privacidade estão comprometidos com uma gestão efetiva de Segurança da Informação na AlmavivA Experience. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da companhia.

2. CAMPO DE APLICAÇÃO

Esta política se aplica a todos os usuários da informação da AlmavivA Experience, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a AlmavivA, tais como prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da AlmavivA e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da AlmavivA Experience.

Cópia Controlada
Reprodução Proibida

3. REFERÊNCIAS

- PPD-001 - Política Externa de Privacidade
- PSI-013 - Política de Segurança da Informação com Fornecedores
- NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.
- NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.
- NBR ISO/IEC 27701:2026 – Segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão da privacidade da informação — Requisitos e orientações.
- Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais).

Cópia Controlada

4. DEFINIÇÕES

- **Segurança da Informação (SI):** Proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade, a disponibilidade e a confidencialidade dessa informação são preservadas. A SI não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do seu uso impróprio. A SI também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias e outros.

- **Privacidade**: Direito do titular de ter seus dados pessoais tratados de forma transparente, segura e em conformidade com a finalidade para a qual foram coletados, conforme legislação vigente.

Reprodução Proibida

5. RESPONSABILIDADES

Compete Diretoria Executiva:

- Promover e aprovar as atividades do Sistema de Gestão de Segurança da Informação e Privacidade.

Compete ao Comitê de Segurança da Informação e Privacidade:

- Conduzir uma avaliação periódica sobre a Segurança da Informação;
- Garantir a disponibilidade dos recursos necessários para uma efetiva gestão de segurança da informação;
- Disseminar a cultura de Segurança de Informação e Privacidade;
- Alinhar os objetivos estratégicos de Segurança da Informação e Privacidade com os objetivos de negócio da AlmavivA Experience;
- Apoiar e aprovar atividades de melhoria contínua do Sistema de Gestão da Segurança da Informação e Privacidade;
- Deliberar sobre aplicação de sanções quando for observado o descumprimento desta política e demais políticas estabelecidas pela área de Segurança da Informação e Privacidade.

Compete aos Colaboradores, Terceiros, Fornecedores e demais partes interessadas pertinentes:

- Cumprir as orientações desta política e demais políticas estabelecidas pela área de Segurança da Informação e Privacidade.
- Zelar pela segurança das informações das empresas, informando quaisquer anormalidades percebidas a área de Segurança da Informação e Privacidade.

Compete à equipe de GRC de Segurança da Informação e Privacidade (GRC):

- Estabelecer as diretrizes de segurança da informação e privacidade.

Cópia Controlada
Reprodução Proibida

- Conscientizar as partes interessadas pertinentes sobre a segurança da informação e privacidade.
- Identificar e reportar os riscos referentes à segurança das informações e Privacidade.
- Estabelecer controles para mitigação dos riscos.
- Manter e melhorar continuamente o sistema de gestão de segurança da informação e privacidade.

Cópia Controlada

6. DIRETRIZES

6.1. DIRETRIZES GERAIS

Esta política demonstra nossa capacidade e integridade em lidar com todas as partes interessadas. Portanto, essa política assegura que:

- As informações estão protegidas contra acesso não autorizado;
- A confidencialidade da informação é mantida;
- Há meios para que as informações não sejam divulgadas às entidades não autorizadas por meio de ações deliberadas ou descuidadas;
- A integridade das informações é mantida para impedir modificações não autorizadas;
- As informações estão disponíveis para usuários autorizados, quando necessário;
- Sempre que ocorrer alterações legais, regulamentares, normativas ou contratuais que impactem o negócio da AlmavivA Experience, uma análise crítica é realizada a fim de que as adequações, se necessário, sejam realizadas;
- Cada indivíduo tenha conhecimento adequado dos controles de gestão, dos controles operacionais e técnicos que ajudam a proteger os recursos e bens tecnológicos de informação da AlmavivA Experience;
- As metas e objetivos são divulgados para as partes interessadas envolvidas, para que haja visão adequada de papeis e responsabilidades em relação à segurança da informação e privacidade e à missão da AlmavivA Experience;
- As políticas, procedimentos e práticas são comunicados às partes envolvidas da AlmavivA Experience, conforme apropriado.

Reprodução Proibida

6.2. REGULAMENTAÇÃO

A AlmavivA Experience e as partes interessadas envolvidas se comprometem a atender integralmente aos requisitos de segurança da informação e privacidade aplicáveis ou exigidos por legislações, regulamentações, estatutos e/ou cláusulas contratuais.

Cópia Controlada

6.3. RISCOS E AMEAÇAS

Todos os ativos de informação e associados devem ser periodicamente avaliados e os respectivos riscos ao negócio da AlmavivA Experience devem ser mapeados.

Os riscos e ameaças inerentes à segurança da informação e privacidade devem ser tratados através da implementação de controles específicos e devem ser periodicamente reavaliados.

O tratamento e monitoramento dos riscos é realizado de acordo com política específica sobre o tema.

6.4. FORNECEDORES

A AlmavivA Experience dispõe de processo de avaliação de riscos dos fornecedores críticos.

Essa metodologia visa detectar, avaliar e gerenciar riscos nos serviços ou produtos prestados por fornecedores e que possam impactar diretamente no negócio da AlmavivA Experience.

Reprodução Proibida

Todos os terceiros devem se comprometer a agir de acordo com a Política de Segurança da Informação e a Política de SI para Fornecedores, ambas publicadas na página da AlmavivA na internet, sendo imprescindível que o contrato firmado entre as empresas possua cláusula que assegure a confidencialidade das informações e a adesão à Política de Segurança da Informação.

6.5. AUDITORIAS

Periodicamente auditorias são realizadas para assegurar a eficácia do Sistema de Gestão de Segurança da Informação e Privacidade e de seus controles, bem como garantir a sua efetiva implementação e manutenção.

Cópia Controlada

6.6. CONTINUIDADE DE NEGÓCIOS

Os planos de continuidade de negócios são produzidos, mantidos e testados de acordo com as expectativas da gestão.

6.7. CLASSIFICAÇÃO DA INFORMAÇÃO

O processo de classificação da informação estabelecido pela AlmavivA Experience tem o objetivo de proteger a informação contra a revelação. Para isso, todo e qualquer tipo de informação criada e/ou armazenada dentro das instalações da empresa deve ser classificada por uma das seguintes opções:

- Pública;
- Interna;
- Restrita;
- Confidencial.

Reprodução Proibida

6.8. TREINAMENTO E CONSCIENTIZAÇÃO

A AlmavivA Experience possui programa de comunicados e treinamentos para os colaboradores.

6.9. TRATAMENTO DE INCIDENTES

Os incidentes de segurança ocorridos na AlmavivA Experience devem ser reportados para área de Segurança da Informação e Privacidade através do e-mail: sip@almavivaexperience.com.br, principalmente os casos de indisponibilidade de sistemas e vazamento de informação de clientes.

Considera-se incidente de Segurança da Informação e Privacidade qualquer evento que tenha impacto na AlmavivA Experience, levando à necessidade de resposta e recuperação. São considerados incidentes de Segurança da Informação e Privacidade ocorrências da seguinte natureza:

Cópia Controlada

- Perda, roubo ou furto de equipamento contendo informações corporativas;
- Mau funcionamento ou sobrecarga de sistema devido a ataques internos ou externos;
- Uso ou acesso à informação sem autorização, seja em formato físico ou digital;
- Não conformidade com políticas e diretrizes de Segurança da Informação e Privacidade;
- Desvio dos controles de Segurança da Informação implantados na AlmavivA;
- Violação de acesso a áreas críticas contendo informações corporativas ou a sistemas.

Os incidentes devem ser priorizados de acordo com a classificação de impacto e criticidade registrados. Dessa forma é possível decidir quando se faz necessário o acionamento do grupo de resposta a incidentes, que por sua vez, decidirá quanto ao acionamento do plano de continuidade de negócios.

6.10. SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE NO GERENCIAMENTO DE PROJETOS

Reprodução Proibida

A Segurança da Informação é integrante participativa da elaboração e entrega de qualquer projeto, especial ou não, que altere o padrão da infraestrutura do ambiente da AlmavivA Experience.

Sendo responsável em avaliar os requisitos ou as necessidades solicitadas, se elas estão em conformidade com os objetivos e diretrizes da Segurança da Informação e estão sendo seguidas em todas as fases dos projetos.

A segurança da informação é responsável em avaliar e identificar os riscos e propor a melhor solução visando atender os objetivos da Segurança da Informação e Privacidade e os objetivos do projeto e/ou negócio.

6.11. DESENVOLVIMENTO SEGURO DE SISTEMAS

O desenvolvimento seguro é um requisito para construir serviço, arquitetura, software e sistema seguros na AlmavivA Experience. Para isso, devem ser considerados minimamente aspectos:

- separação dos ambientes de desenvolvimento, teste e produção;
- segurança no ciclo de vida do desenvolvimento de software:
- requisitos de segurança na fase de especificação e design;
- pontos de verificação de segurança em projetos;
- testes de segurança e aceitação;
- repositórios seguros para código-fonte e configuração;
- segurança no controle de versão;
- conhecimento e treinamento necessários de segurança de aplicações;
- capacidade dos desenvolvedores para prevenir, encontrar e corrigir vulnerabilidade.

Para os testes de sistemas, selecionar, proteger e gerenciar as informações, considerando:

- não replicar informações sensíveis nos ambientes de desenvolvimento e teste do sistema, a menos que sejam fornecidos controles equivalentes para os sistemas de desenvolvimento e teste;
- proteger informações sensíveis por remoção ou mascaramento, quando usadas para testes.

Se o desenvolvimento for terceirizado, deve ser analisada a garantia de que o fornecedor está de acordo com as regras da AlmavivA Experience para o desenvolvimento seguro.

6.12. SEGURANÇA NAS COMUNICAÇÕES

Todas as comunicações entre os ambientes tecnológicos da AlmavivA Experience e as partes interessadas pertinentes devem utilizar canais de comunicações criptografados, utilizando cifras e algoritmos reconhecidamente seguros.

Cópia Controlada
Reprodução Proibida

6.13. CÓPIAS DE SEGURANÇA

Cópias de informações, configuração de softwares e sistemas devem ser mantidas e testadas regularmente de acordo com as políticas específicas sobre backup, permitindo a recuperação de dados ou sistemas, se necessário. Para prevenir o vazamento de dados, devem ser usadas medidas como criptografia, autenticação segura, controle de acesso e proteção física da mídia de armazenamento, quando aplicável.

Cópia Controlada

6.14. PROTEÇÃO E PRIVACIDADE DE DADOS PESSOAIS

Todos os processos existentes na AlmavivA Experience que envolvam o tratamento de dados pessoais devem seguir as diretrizes estabelecidas nas Políticas de Privacidade.

6.15. ANÁLISE CRÍTICA DE SEGURANÇA DA INFORMAÇÃO

Anualmente, ou sempre que surgir uma mudança significativa no modelo de negócio, deve ser realizado um processo formal de análise crítica da política de segurança da informação.

6.16. MELHORIA CONTÍNUA

A melhoria contínua do Sistema de Gestão da Segurança da Informação e Privacidade é um compromisso de todos na AlmavivA Experience e partes interessadas.

Reprodução Proibida

7. DISPOSIÇÕES FINAIS

Qualquer necessidade de ação em desacordo com as regras estabelecidas na Política de Segurança da Informação, na Política de Privacidade e suas políticas complementares devem ser direcionadas à Segurança da Informação para análise do risco, seu registro, e envio para a apreciação pela alçada competente e/ou Comitê de Segurança da Informação e Privacidade.

O colaborador que fizer uso indevido ou não autorizado dos recursos das empresas, violar controle de segurança, ou de qualquer modo agir em desacordo com os termos dessa política,

fica sujeito à aplicação de medidas disciplinares legalmente previstas, podendo haver responsabilização penal, civil e/ou administrativa, na forma da legislação em vigor.

8. ANEXOS

Não se aplica.

Cópia Controlada

Reprodução Proibida