



Política de Segurança da Informação e Segurança Cibernética

Setembro/2026





_sumário

1. Controle do Documento	3
1.1. Identificação	3
1.2. Distribuição e Classificação	3
2. Nosso compromisso	4
3. Princípios que orientam nossa atuação	4
4. Escopo	4
5. Linhas gerais dos controles adotados	5
6. Governança	5
7. Treinamento e conscientização	6
8. Precauções recomendadas a clientes e usuários	6
9. Canal para reporte de incidentes e vulnerabilidades	6
10. Normas de referência	7
11. Aprovação e Responsabilidades	7
12. Histórico de Versões	8



1. Controle do Documento

1.1. Identificação

Campo	Conteúdo
Documento de origem	Política de Segurança da Informação e Segurança Cibernética — AVN-POL-SEGINF-001, versão 2.0
Entidade aplicável	Grupo Avenia
Código	AVN-POL-SEGINF-001-RP
Versão	1.0
Data de emissão	Setembro de 2026
Fundamento da divulgação	Res. BCB 85/2021, art. 5º; Res. CMN 4.893/2021, art. 5º
Frequência de revisão	Sempre que a versão vigente da Política sofrer alteração relevante é, no mínimo, anual
Classificação	Público — divulgação externa

1.2. Distribuição e Classificação

Este documento é classificado como **público — divulgação externa**. É disponibilizado a clientes, usuários, parceiros e ao público em geral por meio dos canais oficiais da Avenia, em atendimento ao dever de divulgação previsto na Res. BCB 85/2021, art. 5º, e na Res. CMN 4.893/2021, art. 5º. Este resumo não substitui a Política de Segurança da Informação e Segurança Cibernética integral (AVN-POL-SEGINF-001), classificada como confidencial — uso interno, cujo acesso é restrito a colaboradores, prestadores de serviços e terceiros autorizados, bem como a autoridades regulatórias competentes e auditores externos. A reprodução deste resumo é permitida desde que preservadas a integridade do conteúdo e a indicação da fonte.



2. Nosso compromisso

A Avenia trata a segurança da informação e a segurança cibernética como pilares da confiança que clientes, parceiros e reguladores depositam em nossos produtos. Como grupo dedicado a infraestrutura financeira baseada em *stablecoins*, câmbio e pagamentos transfronteiriços, protegemos ativos de informação, dados de clientes e a continuidade dos serviços com controles proporcionais à sensibilidade das operações.

Este documento é o **resumo público** da nossa Política de Segurança da Informação e Segurança Cibernética, publicado em atendimento à Res. BCB 85/2021, Art. 5º e à Res. CMN 4.893/2021, Art. 5º. A versão integral é de uso interno.

3. Princípios que orientam nossa atuação

- **Confidencialidade, integridade e disponibilidade** dos ativos de informação sob nossa responsabilidade.
- **Proteção de dados pessoais** em conformidade com a Lei Geral de Proteção de Dados (Lei 13.709/2018) e demais legislações aplicáveis, incluindo o Regulamento Geral de Proteção de Dados europeu (GDPR) quando aplicável.
- **Proporcionalidade** entre medidas de segurança e a criticidade dos ativos, sistemas e dados envolvidos.
- **Melhoria contínua**, com revisões periódicas da política, dos controles e dos planos de resposta.
- **Cultura de segurança**, estendida a todos os administradores, colaboradores, prestadores de serviços, fornecedores e parceiros de negócio.

4. Escopo

A Política aplica-se a todas as pessoas que atuem, direta ou indiretamente, em processos, sistemas ou operações da Avenia — administradores, colaboradores, prestadores de serviços, terceirizados, fornecedores e demais parceiros —, cobrindo os ambientes tecnológicos, físicos e humanos que sustentam nossos produtos.



5. Linhas gerais dos controles adotados

Sem detalhar arquiteturas ou ferramentas específicas, mantemos, entre outros:

- **Gestão de identidade e acesso** — autenticação robusta, incluindo múltiplos fatores para acessos sensíveis, e aplicação do princípio do menor privilégio, com revisão periódica de permissões.
- **Segmentação de ambientes e proteção de rede** — separação lógica entre ambientes produtivos e não produtivos e controles de tráfego em pontos críticos.
- **Criptografia em trânsito e em repouso** — proteção de comunicações, bases de dados e cópias de segurança por meio de padrões criptográficos reconhecidos e gestão controlada de chaves.
- **Gestão de riscos e vulnerabilidades** — avaliações periódicas, tratamento formal de riscos, testes e programa contínuo de remediação.
- **Continuidade de negócios** — cópias de segurança periódicas, testes de restauração e ambiente de recuperação de desastres que suportam a retomada dos serviços críticos.
- **Segurança física** — controle de acesso a instalações relevantes, monitoramento e proteção ambiental.
- **Segurança em serviços de nuvem e de terceiros** — avaliação prévia de fornecedores relevantes, requisitos contratuais de segurança, direito de auditoria e monitoramento contínuo, em linha com os requisitos das Res. BCB 85/2021 e Res. CMN 4.893/2021 para contratação de serviços relevantes de processamento e armazenamento de dados e computação em nuvem, inclusive no exterior.
- **Rastreabilidade e monitoramento** — registro de eventos relevantes de segurança e mecanismos de auditoria para apoiar detecção e investigação de incidentes.
- **Gestão de incidentes** — processos para detecção, registro, tratamento, comunicação e análise de causa e impacto de incidentes, incluindo comunicação a autoridades competentes e partes afetadas quando aplicável.

6. Governança

A Política é aprovada pela Diretoria Executiva da Avenia, com revisão no mínimo anual e sempre que ocorra mudança regulatória, tecnológica ou evento relevante que a justifique. A Diretoria Responsável por Tecnologia conduz a manutenção da política, a gestão de exceções na sua alçada e a interlocução com auditores e reguladores. Áreas de Tecnologia e



Segurança da Informação, Riscos, Compliance, Jurídico e Auditoria Interna possuem papéis definidos no ciclo de identificação, tratamento e monitoramento de riscos e incidentes.

Exceções à política são formalizadas, justificadas, temporárias e submetidas à aprovação do Comitê de Tecnologia e Segurança da Informação, com controles compensatórios e prazo de expiração.

7. Treinamento e conscientização

A Avenia promove, de forma contínua, capacitação e ações de conscientização para todos os administradores e colaboradores em temas de segurança da informação, proteção de dados, prevenção a fraudes e resposta a incidentes, alinhadas às funções desempenhadas por cada profissional. Fornecedores e parceiros são informados dos requisitos aplicáveis por meio contratual e operacional.

8. Precauções recomendadas a clientes e usuários

Como boas práticas para utilização segura de produtos e serviços da Avenia, recomendamos, entre outras:

- Utilizar senhas fortes e exclusivas em cada serviço e ativar, sempre que disponível, mecanismos de autenticação de múltiplos fatores.
- Manter dispositivos, sistemas operacionais e aplicativos atualizados.
- Desconfiar de mensagens não solicitadas (e-mails, aplicativos de mensagem, ligações) que solicitem credenciais, chaves privadas, códigos de verificação, transferências ou instalação de aplicativos.
- Nunca compartilhar chaves privadas, *seed phrases*, senhas ou códigos de autenticação com terceiros, incluindo pessoas que se apresentem como representantes da Avenia.
- Acessar nossos serviços exclusivamente por meio dos canais oficiais divulgados pela Avenia.
- Comunicar imediatamente à Avenia qualquer suspeita de acesso indevido, fraude ou vazamento envolvendo sua conta ou informações.

9. Canal para Reporte de Incidentes e Vulnerabilidades

Suspeitas de incidentes, vulnerabilidades ou uso indevido envolvendo os produtos, sistemas ou canais da Avenia podem ser comunicadas pelo endereço



cybersecurity@avenia.io. As comunicações são tratadas com confidencialidade e encaminhadas às áreas responsáveis.

10. Normas de Referência

A Política de Segurança da Informação e Segurança Cibernética da Avenia observa, entre outras referências aplicáveis:

- **Res. BCB 85/2021** — política de segurança cibernética e contratação de serviços de processamento, armazenamento de dados e computação em nuvem para instituições de pagamento.
- **Res. CMN 4.893/2021** — política de segurança cibernética e contratação de serviços de processamento, armazenamento de dados e computação em nuvem para instituições financeiras.
- **Lei 13.709/2018 (LGPD)** e demais normas aplicáveis de proteção de dados pessoais.

Este resumo público é atualizado sempre que a versão vigente da Política sofrer alteração relevante. Última atualização: setembro de 2026.

11. Aprovação e Responsabilidades

Função	Responsável	Atribuição
Diretor responsável	<i>Chief Technology Officer</i>	Manutenção do resumo e garantia de aderência à Política integral vigente
Elaboração	Tecnologia da Informação	Consolidação do conteúdo a partir da Política integral, sem exposição de detalhes sensíveis
Revisão de conformidade	Compliance	Aderência regulatória e adequação do conteúdo à divulgação pública
Aprovação	Diretoria Executiva	Aprovação formal em ARD
Publicação	Tecnologia da Informação	Disponibilização e atualização no site da Avenia



12. Histórico de Versões

Versão	Data	Autor	Descrição da Alteração
1.0	Setembro de 2026	Tecnologia da Informação	Emissão inicial do resumo público, com base na versão 2.0 da Política (AVN-POL-SEGINF-001)