





# **Política de Segurança da Informação e Cibernética**

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

## SUMÁRIO

<b>1. OBJETIVO .....</b>	<b>3</b>
<b>2. ABRANGÊNCIA.....</b>	<b>3</b>
<b>3. DIRETRIZES .....</b>	<b>3</b>
<b>4. PARCEIROS E FORNECEDORES.....</b>	<b>4</b>
<b>5. RESPONSABILIDADES.....</b>	<b>6</b>
5.1. CONSELHO DE ADMINISTRAÇÃO .....	6
5.2. DIRETORIA EXECUTIVA .....	7
5.3. TECNOLOGIA DA INFORMAÇÃO.....	7
<b>6. DISPOSIÇÕES FINAIS .....</b>	<b>7</b>

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

## 1. Objetivo


Essa política orienta na gestão da segurança da informação e cibernética, demonstrando o compromisso com a proteção das informações corporativas e demais ativos de informação. Ela compõe a relação de políticas associadas à gestão de continuidade de negócio do AL5 Bank.

## 2. Abrangência

A Política de Segurança da Informação e Cibernética (PSIC) aplica-se a todos os usuários, sistemas e ambientes corporativos, fornecedores e prestadores de serviços que atuam no AL5 Bank.

## 3. Diretrizes

- a) Tratamos a informação, na gestão empresarial, como ativo;
- b) Alinhamos a gestão da segurança da informação e cibernética aos nossos negócios;
- c) Realizamos o tratamento da informação em todo seu ciclo de vida de modo ético e responsável;
- d) Garantimos a confidencialidade, integridade e disponibilidade da informação;
- e) Aplicamos proteção aos ativos de informação de forma compatível com sua criticidade para nossas atividades, alcançando todos os processos, informatizados ou não, inclusive quando do uso de computação em nuvem;
- f) Identificamos, analisamos, avaliamos e tratamos os riscos que envolvam os ativos de informação, por meio de avaliações periódicas, a intervalos regulares;
- g) Adotamos mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens, e roubo e ataques cibernéticos, em todo o ciclo de vida das informações;
- h) Monitoramos de forma contínua os ativos de informação e utilizamos processos, controles e tecnologias de prevenção e resposta a ataques cibernéticos;
- i) Obedecemos ao princípio de segregação das funções de desenvolvimento e uso dos ativos da informação, na gestão da segurança da informação e cibernética;
- j) Procedemos à identificação e definição de, pelo menos, um gestor da informação e atribuímos-lhe responsabilidades sobre a informação em todo o seu ciclo de vida;

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

- k) Disseminamos a cultura de segurança da informação e cibernética por meio de programa permanente de sensibilização, conscientização e capacitação;
- l) Preservamos nossos requisitos de segurança da informação e cibernética na contratação de serviços ou de pessoas e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários;
- m) Concedemos a funcionários e terceiros somente o acesso às informações necessárias ao desempenho de suas funções e atribuições previstas em contrato ou por determinação legal;
- n) Identificamos, por meio do controle de acesso, cada usuário individualmente e nos casos devidamente comprovados de tratamento indevido da informação corporativa o responsabilizamos, juntamente com o administrador que lhe concedeu o acesso;
- o) Analisamos as ocorrências de tratamento indevido de informações corporativas sob os aspectos legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo as vulnerabilidades.


#### **4. Parceiros e Fornecedores**

Sem prejuízo das condições contratuais e das condutas de boas práticas esperadas, o terceiro obriga-se a estabelecer e evidenciar ao AL5 BANK quando solicitado:


- a) a política de segurança da informação adotada pela empresa;
- b) as políticas, diretrizes e planos de gerenciamento de incidentes da segurança da informação, o fluxo de comunicação com a Instituição, medidas para detecção, prevenção e correção do incidente, além da definição dos responsáveis pelos danos causados à Instituição;
- c) o Plano de Continuidade de Negócios, o qual deve contemplar como se dará a continuidade de suas operações, principalmente as atividades, incluindo contingência de funcionamento e os planos de recuperação de desastre e diretrizes de resiliência.

Sem prejuízo das condições contratuais e das condutas de boas práticas esperadas, recomenda-se que o terceiro:

- a) defina, formalmente, os funcionários de alta gestão envolvidos na execução das atividades objeto do contrato, bem como seus papéis e responsabilidades;
- b) proteja a informação recebida por força do contrato contra a interceptação, cópia, modificação não autorizada, indisponibilidade, desvio e destruição;

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

- c) acolha assinatura de todos os empregados que venham a ter acesso à informação corporativa do AL5 Bank durante a execução do contrato em termo(s) específico(s) a ser fornecido pelo gestor do contrato;
- d) guarde sigilo do Código de Usuário e demais credenciais de acesso a que venha a receber do AL5 Bank, para acesso aos seus ativos de informação, podendo vir a responder cível ou penalmente por qualquer quebra de segurança decorrente de seus atos;
- e) formalize os procedimentos de custódia das informações corporativas, entregues pelo AL5 BANK para a execução das atividades, com definição clara dos usuários e custodiantes que a elas terão acesso;
- f) mantenha programa de educação, treinamento e conscientização sobre segurança da informação para funcionários que tiverem acesso às informações corporativas do AL5 BANK;
- g) oriente os funcionários envolvidos na execução do contrato quanto à confidencialidade, integridade e disponibilidade das informações corporativas do AL5 Bank;
- h) atente para a observância do direito autoral e da propriedade intelectual nos recursos (físicos ou tecnológicos) empregados na execução do contrato;
- i) proteja as correspondências, físicas ou eletrônicas, transitadas durante a execução das atividades, observando-se a regulamentação legal nacional e internacional, quando aplicável;
- j) adote precauções, medidas e controles para manutenção da confidencialidade, integridade e disponibilidade da informação em qualquer meio (falada, impressa, por imagens, vídeos, outros) nos ambientes de execução do contrato;
- k) relacione, nos casos em que o contrato não dispor o contrário, todas as informações corporativas do AL5 BANK, recebidas ou armazenadas em virtude do contrato, para devolução ou comprovação da sua destruição ao seu termo;
- l) identifique e segregue os dados dos clientes do AL5 BANK por meio de controles físicos ou lógicos;
- m) atente para a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do AL5 BANK;
- n) obtenha, nos casos em que houver previsão contratual de “quarteirização” das atividades ou ações ligadas ao contrato, autorização do AL5 BANK antes de franquear as informações corporativas;
- o) exija de toda a cadeia de suprimento o atendimento aos critérios de segurança da informação;

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

- p) consulte formalmente o gestor do contrato nos casos de surgimento de situações atípicas e que gerem dúvidas sobre a aplicabilidade de controles de segurança da informação.

Conforme disposto na Resolução CMN nº 4.893/2021, a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve observar os seguintes requisitos:


- a) Cumprimento da legislação e da regulamentação em vigor;
- b) Aderência a certificações exigidas para a prestação do serviço a ser contratado;
- c) Acesso aos dados e às informações a serem processados ou armazenados;
- d) Provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- e) Adoção de medidas de segurança para a transmissão e armazenamento de dados;
- f) Obrigação de a empresa contratada manter o AL5 BANK permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- g) Para serviço prestado no exterior, é necessária a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados.

## 5. Responsabilidades

Todos os profissionais notadamente dentro de suas correspondentes atividades têm funções e responsabilidade relacionadas à Política de Segurança da Informação e Cibernética.

### 5.1. Conselho de Administração

- a) Garantir a revisão periódica desta política, bem como a sua aprovação e divulgação a todos os colaboradores da instituição;
- b) Determinar as diretrizes institucionais com base em valores e princípios estabelecidos na presente Política, nas normas de controles internos, nas normas emanadas dos órgãos e entidades de regulação e nas melhores práticas aplicáveis;
- c) Deliberar sobre os casos omissos à esta política.

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

## 5.2. Diretoria Executiva

- a) A Diretoria é patrocinadora dessa Política, sendo responsável por assegurar que o programa receba suporte adequado;
- b) Garantir a conscientização de todos os colaboradores quanto à importância de suas atividades e de como elas contribuem para atingir os objetivos estratégicos definidos para a segurança da informação e segurança cibernética;
- c) Garantir a disponibilização dos recursos necessários para cumprimento desta política.

## 5.3. Tecnologia da Informação


Área responsável por gerir e direcionar as ações de segurança da informação e cibernética no AL5 Bank. A TI em conjunto com a Diretoria de Clientes e Produtos, devem definir e documentar a PSIC, seus procedimentos e garantir que os controles estabelecidos por estes documentos sejam implementados adequadamente. Além disso, a TI possui as seguintes responsabilidades:

- a) Garantir que haja monitoramento e análise de alertas de segurança da informação e segurança cibernética, direcionando as ações necessárias para as equipes/áreas apropriadas;
- b) Desenvolver e disseminar ações de conscientização em Segurança da Informação para todos os usuários do AL5 Bank;
- c) Analisar o resultado de auditorias relacionadas à Segurança da Informação e medir a eficácia dos controles estabelecidos pela respectiva Política;
- d) Garantir melhorias nos processos da PSIC para atingir os objetivos estratégicos a estes relacionados;
- e) Conhecer, cumprir e fazer cumprir em suas atividades as diretrizes e orientações estabelecidas nesta PSIC, bem como acompanhar e observar o cumprimento dos contratos.

## 6. Disposições Finais

Todos os colaboradores são individualmente responsáveis por assegurar o cumprimento deste documento em complementaridade com o Código de Ética e Conduta e com as legislações e regulamentações vigentes.

Os superiores imediatos deverão garantir que os seus subordinados recebam orientação necessária para atenderem os requisitos deste documento.

Título <b>Política de Segurança da Informação e Cibernética</b>		
Número do Documento <b>CA0020</b>	Revisão <b>04</b>	

---

Toda e qualquer situação, que não esteja contemplada neste documento, será analisada e orientada pela área de Tecnologia de Informação.

A revisão ou revalidação deste documento deverá ser realizada anualmente, a partir da data de sua efetiva aprovação. Em casos de alterações na legislação vigente e mudanças na estrutura organizacional ou em processos do AL5 Bank, os responsáveis poderão, a qualquer momento, iniciar o processo de atualização.

A área Tecnologia de Informação é a responsável pela emissão deste documento, e a sua aprovação deve ser atribuída ao nível hierárquico definido no documento CA0008 - Política de Hierarquia de Documento Normativo.