
# POLÍTICA DE SEGURANÇA CIBERNÉTICA

*Versão: 2025.1*
*Data Aprovação: 16/10/2025*
*Aprovação: DIRETORIA*

## 1. OBJETIVO

Esta política tem por objetivo estabelecer os fundamentos associados ao processo de segurança cibernética definidos com base em princípios e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade de dados e de computação em nuvem, em conformidade com a Resolução BCB n° 85/2021 e Resolução BCB nº 368/2024.

## 2. CONCEITO

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Alguns outros conceitos são essenciais para a compreensão do processo, assim definidos:

I. Confidencialidade: Garantir que as informações sejam acessadas apenas por pessoas autorizadas;

II. Integridade: Garantir que as informações, tanto em sistemas quanto em bancos de dados, verdadeiro e correto para seus propósitos originais;

III. Integridade: Garantir que as informações, tanto em sistemas quanto em bancos de dados, verdadeiro e correto para seus propósitos originais;

IV. Disponibilidade: Garantir que as informações e os recursos estejam disponíveis para aqueles que precisam deles quando necessário;

V. Ataques Cibernéticos: Os ataques cibernéticos mais comuns, podem ser realizados através de software maliciosos que são desenvolvidos para corromper computadores e redes de dados, que podem ser realizados através de métodos de manipulação para obtenção de informações confidenciais, como senhas e dados pessoais, ou que possa visar a negação ou atraso de acessos aos serviços ou sistemas da instituição;

VI. Incidente de Segurança da Informação: O incidente de segurança da informação pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança, que pode comprometer a Confiabilidade, Integridade e/ou Indisponibilidade da informação.

## 3. PRINCÍPIOS

A proteção e privacidade dos dados dos clientes refletem os valores da COLUNA, a qual reafirma o seu compromisso com a melhoria contínua da eficácia do processo de proteção de dados.

Quanto as informações dos clientes, deve-se observar as seguintes determinações:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente serão acessados por pessoas autorizadas e capacitadas para o uso adequado;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

## 4. ESTRUTURA ORGANIZACIONAL

Na COLUNA são adotados modelos de estrutura descentralizada a fim de assegurar isenção ou potenciais conflitos de interesses.

## 5. RESPONSABILIDADES

Em linha com o escopo desta política, seguem abaixo transcritas os papéis e responsabilidades detalhados e segmentados.

### 5.1. DIRETORIA

- Revisar e atualizar esta Política anualmente ou quando necessário, em conjunto com as demais áreas integrantes;
- Deliberar sobre as decisões e ações relacionadas à segurança cibernética;
- Monitorar ativamente e tratar dos assuntos referentes ao tema em nível estratégico, tático e operacional;
- Conduzir o processo de investigação interna e apuração de causas e responsabilidades nos incidentes ou violações de segurança;
- Monitorar ativamente a observância dos dispositivos contidos nesta Política;
- Definir procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;

Fazer constar sua responsabilidade pelas informações divulgadas no relatório anual de acesso público, evidenciando a estrutura de gerenciamento desses riscos.

### 5.2. TECNOLOGIA INFORMAÇÃO

- Definir procedimentos e controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética e publicá-los em documento interno específico para seu registro;
- Atualizar regras e procedimentos técnicos referentes a prevenção e proteção de ativos de tecnologia;
- Registrar e analisar a causa e o impacto, bem como controlar os efeitos de incidentes relevantes para as atividades da instituição e publicá-los em documento interno específico para seu registro;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes e publicá-los em documento interno específico para seu registro;
- Manter soluções de prevenção e proteção de dados sempre atualizadas;
- Proteger os dados através de backups periódicos;

- Realizar diligência na contratação de serviços de terceiros, inclusive serviços em nuvem;

- Avaliar questões de segurança durante as fases de pré-projeto e desenvolvimento de novos sistemas, softwares ou aplicações.

### 5.3. COMPLIANCE

- Aplicar Treinamento referente ao conteúdo desta política, sempre que necessário;

- Propor sugestões para a correção tempestiva de deficiências e fraquezas eventualmente identificadas nesse processo, ou ajustes decorrentes de exigências e alterações requeridas pelo Banco Central.

### 5.4. GESTORES ÁREAS

- Disseminar aos colaboradores sob sua gestão, a política, controles, procedimentos e padrões que eles deverão seguir e respeitar;

- Responsabilizar-se pela propriedade das informações de sua área ou quando a classificação da informação assim exigir.

### 5.5. DEMAIS COLABORADORES

- Respeitar e cumprir todo o conteúdo disposto nesta política e nas demais políticas do Grupo;

- Ter ciência de que todas as informações geradas, acessadas, processadas, utilizadas ou armazenadas em qualquer meio ou sistema de informação, devem ser exclusivas as atividades na COLUNA;

- Reportar para as áreas responsáveis qualquer violação ou incidente de segurança da informação;

- Participar dos treinamentos e disseminar a cultura e importância de todos agirem com responsabilidade no tratamento das informações.

## 6. DIRETRIZES

Assegurar que as informações sejam adequadamente protegidas, através dos processos e controles.

### 6.1. Controle de Segurança Cibernética

Os controles de segurança cibernética, devem estar alinhados e acordados entre a estrutura da instituição.

- Bancos de dados e dispositivos de rede com segurança dedicada que seja rigorosamente controlado para preservar a integridade, a confidencialidade e a disponibilidade do conteúdo;

- Manutenção e atualização dos sistemas operacionais e softwares utilizados na instituição;

- Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores dos sistemas/redes, filtros de spam, controle para uso de periféricos, soluções de prevenção e correções de vulnerabilidades e filtros de uso de internet;

- Inclusão das preocupações de segurança durante as fases de desenvolvimento de novos sistemas, softwares ou aplicações;

- Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acessos.

### 6.2. Concessão de Acesso a Usuários, Registro, Manutenção e Verificação Periódica

Em função da amplitude dos acessos dos colaboradores que implementam e mantém a infraestrutura de tecnologia, sua contratação deve ser formalizada considerando a validação de perfil e idoneidade comprovados, e formalizado o seu direito de acesso e comprometimento com o sigilo de informações declarado em documento próprio, que autorize o monitoramento integral de suas atividades e comunicação, além de aceitar a responsabilidade sobre as ações que perpetrar no exercício das suas funções.

As funções de segurança exercidas pelos responsáveis pela Infraestrutura (Software e Hardware) são sujeitas a geração de Logs de atividades que serão armazenados de forma protegida e terão revisão independente pelo Gestor TI.

### 6.3. Registro, Proteção e Revisão de Registro de Eventos (Logs)

Os Sistemas, utilitários como gerenciadores de banco de dados e outras ferramentas de gestão de rede, especialmente as que acessam dados em produção, geram registro de operações sensíveis feitas pelo Suporte/Gestão de Infra, é fundamental que este Log seja mantido protegido de alteração e deleção.

Deverá ser feita revisão periódica deles, quer diretamente, quer usando rotina de extração de operações pontuais com software de extração e análise de dados.

### 6.4. Rotinas Não-Estruturadas

As rotinas que acessem ou alterem banco de dados e outros arquivos de informações, deverão ser mantidos os requisitos mínimos de controle como: Backup, limitação de uso, retenção de fontes e forte monitoramento de rotinas usadas no ambiente de produção, mediante a aprovação do Gestor de TI.

### 6.5. Testes de Contingência

A efetividade da Política, deve ser verificada por meio de testes e revisões periódicas dos controles existentes.

O plano de teste deve ser executado pela área de Tecnologia da Informação assegurando que:

- Os acessos dos colaboradores estão em conformidade com os acessos as áreas de atuação;

- Que os níveis de confidencialidade e acessos as informações confidenciais estão adequadas;

- Recursos computacionais de controle de acesso físico e lógico, estejam protegidos;

- Definição de parâmetros para avaliação dos controles de vulnerabilidade;
- Que haja rastreabilidade de registros que permitam a realização de auditorias periódicas.

### 6.6. Processamento, Armazenamento de Dados e Computação Nuvem

A contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a COLUNA , assegura-se um procedimento efetivo para a aderência às regras previstas na regulamentação vigente.

### 6.7. Recomendações de Segurança aos Clientes

A instituição adotará medidas para conscientizar e orientar seus clientes e usuários sobre os riscos associados à segurança cibernética, observando as diretrizes da Resolução BCB nº 85/2021 e práticas de mercado.

As recomendações incluirão, entre outras:

- incentivo à adoção de boas práticas de segurança da informação, tais como uso de senhas fortes, atualização de sistemas e cautela com links ou mensagens suspeitas;
- alertas regulares sobre fraudes eletrônicas, golpes e incidentes de segurança divulgados por órgãos oficiais e pela própria instituição;
- disponibilização, em meio eletrônico de fácil acesso (website e canais oficiais), de material educativo atualizado sobre segurança digital e prevenção a incidentes.

A Diretoria responsável assegurará que as comunicações sejam claras, compreensíveis e alinhadas às orientações de segurança cibernética estabelecidas pela instituição.

### 6.8. Canal de Denúncias – Segurança Cibernética

A instituição manterá canal de comunicação específico, permanente e de fácil acesso, destinado ao recebimento de comunicações e denúncias relacionadas a incidentes de segurança cibernética, bem como suspeitas de violação de dados ou condutas irregulares.

O canal deverá:

- possibilitar o registro de denúncias identificadas ou anônimas, preservando o sigilo das informações;
- garantir tratamento tempestivo e adequado das comunicações recebidas, com registro formal e encaminhamento às áreas competentes;
- integrar-se ao processo de gerenciamento de riscos operacionais e de continuidade de negócios, nos termos da Resolução BCB nº 265/2022;
- permitir o acompanhamento da resolução dos incidentes reportados e comunicação à Diretoria responsável.

A administração assegurará que o canal de denúncias seja amplamente divulgado a todos os colaboradores, parceiros, fornecedores e clientes da instituição.

## 7. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Em casos de ocorrência de um incidente de segurança da informação, a tratativa poderá ser conduzida das seguintes formas:

- Incidente técnico relacionado a qualquer tipo de ameaça ou vulnerabilidade deverá ser tratado através de procedimento com o papel fundamental de agir e mitigar o incidente o mais rápido possível;

- Incidentes comportamental deverá ser reportado para a área de Compliance que analisará caso a caso e adotará as medidas cabíveis conforme estabelecido na Política de Segurança da Informação.

## 8. PENALIDADES

O descumprimento de alguma regra desta política será considerado como falta grave, conforme disposto nos Código de Ética e Conduta da COLUNA ou de acordo com análise de decisão de Comitê de Compliance, sujeitando o Colaborador a sanções administrativas de acordo com o grau de severidade do incidente.