

# ***Rendimento/***

Resumo da Política de Segurança da Informação e  
Cibernética

# Sumário

<b>1. Objetivo</b> .....	2
<b>2. Público Alvo</b> .....	2
<b>3. Papéis e Responsabilidades</b> .....	2
<b>4. Conceito e Diretrizes de Segurança</b> .....	3
<b>5. Referências Normativas</b> .....	3
<b>6. Controle de Versão</b> .....	4

## 1. Objetivo

Estabelecer um conjunto de diretrizes e regras para proteger os ativos de informação do **GRUPOBRSA** contra ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade de dados e sistemas, minimizando riscos e atendendo as legislações e regulamentações vigentes.

## 2. Público-alvo

Esta Política se aplica a todos os colaboradores, que possuam acesso às informações do **GRUPOBRSA**.

## 3. Papéis e Responsabilidades

### **Alta Administração e Governança:**

O tema é gerido de forma estratégica, contando com um Diretor responsável pela Segurança Cibernética e um Comitê de Segurança da Informação, encarregados de aprovar investimentos, promover a cultura de segurança e garantir o alinhamento com os objetivos do negócio.

### **Áreas de Defesa e Controle:**

Equipes dedicadas de Segurança da Informação, Tecnologia da Informação (TI), Riscos, Compliance e Auditoria atuam em conjunto para avaliar riscos, monitorar ameaças, implementar controles tecnológicos (como firewalls, antivírus e criptografia) e validar a eficácia contínua das proteções implementadas.

### **Gestores e Colaboradores:**

A proteção dos dados é uma responsabilidade compartilhada. Todos os usuários dos ativos de informação devem atuar de forma ética, zelar pelo sigilo das senhas, adotar boas práticas (como mesa e tela limpas) e reportar imediatamente qualquer atividade suspeita.

#### 4. Conceito e Diretrizes de Segurança

O **GRUPOBRSA** adota premissas rígidas para o gerenciamento de seu ambiente, destacando-se os seguintes conceitos globais aplicados à nossa operação:

- **Gestão de Riscos e Classificação da Informação:** Os riscos cibernéticos são continuamente avaliados em novos produtos, serviços e processos corporativos. A informação é classificada e tratada com o devido rigor, alinhada aos preceitos de privacidade e proteção de dados pessoais (LGPD).
- **Controle de Acessos:** A concessão de acessos lógicos e físicos é baseada no princípio do "privilegio mínimo" e na necessidade da função. Os acessos externos e remotos ocorrem exclusivamente por meio de canais seguros, criptografados e autenticados (VPNs).
- **Proteção de Redes e Ativos:** Nossos ambientes lógicos são segregados e monitorados de forma ininterrupta por um Centro de Operações de Segurança (SOC) 24/7, garantindo a identificação ágil e o bloqueio de atividades suspeitas em tempo real. Todos os ativos de tecnologia passam por rígida gestão de configuração e atualizações de segurança.
- **Gestão de Terceiros e Nuvem:** Prestadores de serviços relevantes e provedores de computação em nuvem passam por diligência prévia (Due Diligence), devendo comprovar conformidade com os nossos requisitos de segurança e com as normas regulatórias antes e durante a vigência do contrato.
- **Continuidade de Negócios e Respostas a Incidentes:** O GRUPOBRSA mantém processos de backup para a salvaguarda de dados e Planos de Continuidade de Negócios que contemplam cenários de incidentes cibernéticos. Possuímos equipes treinadas para registrar, analisar e responder a incidentes de segurança cibernética visando a rápida mitigação e restauração da normalidade.
- **Conscientização:** Mantemos programas contínuos de treinamento e disseminação da cultura de segurança da informação para todos os nossos profissionais.

#### 5. Referências Normativas

- Resolução 4.893 de 26 de fevereiro de 2021 e Resolução N°85 de 8 de abril de 2021 do Banco Central do Brasil que, dispõe sobre a Política de Segurança Cibernética.
- Resolução CMN n° 5.274, de 18 de dezembro de 2025 – Altera a Resolução 4.893/2021, atualizando e aprimorando as diretrizes da Política de Segurança Cibernética.
- Resolução BCB n° 368 de 25/1/2024.
- Circular n° 3978/20 – Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei n° 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei n° 13.260, de 16 de março de 2016.

## 6. Controle de Versão

Versão	Data de Atualização	Conteúdo Revisado
1	Abril de 2026	Elaboração pelo Departamento de Segurança da Informação