

Política de Segurança da Informação, Cibernética e Proteção de Dados Pessoais

Versão [●]

**Política de Segurança da Informação, Cibernética
e Proteção de Dados Pessoais**

| Versão | Data de Aprovação | Validação Técnica (cargo/nome) |
|---------------|--------------------------|---------------------------------------|
| [.] | [.] | [.] |
| [.] | [.] | [.] |

I. OBJETIVO

A BRADO CAPITAL mantém Política de Segurança da Informação, Cibernética e Proteção de Dados Pessoais ("Política") com a finalidade proteger os equipamentos, sistemas e dados de propriedade e/ou uso da BRADO CAPITAL contra o uso indevido, fraudes, ataques de hackers, perda ou sequestro de dados.

II. SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

1.1. Diretrizes Gerais de Segurança da Informação

Esta Política tem como diretrizes básicas:

- (i) Assegurar a confidencialidade, integridade e disponibilidade das informações da BRADO CAPITAL, mediante utilização de mecanismos de Segurança da Informação e Cibernética, balanceando fatores de risco, tecnologia e custo;
- (ii) Garantir a proteção adequada das informações e dos sistemas contra acesso indevido, cópia, leitura, modificação, destruição e divulgação não autorizados;
- (iii) Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela BRADO CAPITAL, estando sujeitos à monitoração, rastreabilidade e auditoria;
- (iv) Assegurar a participação dos colaboradores da BRADO CAPITAL em treinamentos para conscientização sobre segurança da informação e cibernética;
- (v) Assegurar a existência de processos de continuidade de negócios e gestão de incidentes de segurança para proteção, detecção, resposta e recuperação contra ataques cibernéticos, comunicando, em caso de incidentes, os titulares dos dados pessoais envolvidos e autoridades competentes, de acordo com as leis e regulamentações em vigor;
- (vi) Informar aos clientes e terceiros sobre as precauções de Segurança da Informação e Cibernética necessárias na utilização de produtos e serviços financeiros ofertados pela BRADO CAPITAL;
- (vii) Garantir o cumprimento desta Política e demais normas relacionadas;

(viii) Assegurar o comprometimento da alta administração com a melhoria contínua dos processos e recursos necessários para Segurança da Informação e Cibernética.

1.2. Princípios Básicos de Segurança da Informação

- **Autenticidade:** garante que a informação é proveniente da fonte anunciada;
- **Confidencialidade:** garante que a informação seja acessível apenas por agentes autorizados e dela se utilizem estritamente para o desempenho de suas funções na qualidade de colaborador da BRADO CAPITAL, impedindo que a informação se torne pública ou acessível a qualquer terceiro que esteja fora da BRADO CAPITAL;
- **Integridade:** garante que a informação seja mantida em seu estado original desde sua criação, protegendo durante a guarda ou transmissão contra alterações indevidas, intencionais ou acidentais até o descarte, se aplicável;
- **Disponibilidade:** garante que a informação e os serviços essenciais estarão disponíveis para os usuários quando requeridos;
- **Não repúdio:** capacidade de identificar uma ação já executada, de forma que o executor não possa negar a autoria;

2. Gestão de Riscos

Todos os produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados devem ser submetidos a um processo formal de análise, avaliação e tratamento de riscos, visando atingir o grau de segurança adequado para a BRADO CAPITAL.

3. Gestão de Continuidade

A BRADO CAPITAL deve implementar planos de continuidade de negócios documentados, testados e revisados periodicamente, de forma que seus serviços essenciais sejam devidamente identificados, contemplando os mecanismos de segurança da informação estabelecidos nos ambientes de produção.

Deve haver redundância dos ativos, para que atendam aos requisitos de disponibilidade.

4. Gestão De Incidentes De Segurança Da Informação E/Ou Privacidade

Todos os Colaboradores devem reportar quaisquer incidentes de segurança, para que estes possam ser classificados, analisados, monitorados, comunicados e devidamente tratados conforme seu nível de criticidade.

5. Classificação da Informação

As informações da BRADO CAPITAL somente poderão ser utilizadas em cumprimento aos propósitos de negócios e o acesso dependerá da função exercida e da autorização prévia do responsável pela informação.

Todas as informações devem ser classificadas com base em sua sensibilidade para o negócio.

6. Gestão de Acessos

No ato da contratação, mudança de área ou desligamento de Colaboradores ou finalização do vínculo de Terceiros, devem existir processos que registrem, revisem e ajustem os acessos físicos e lógicos de acordo com as novas funções desempenhadas, para garantir os acessos somente as informações e recursos necessários ao seu novo cargo ou função.

6.1. Senhas de Usuários

Todas as senhas dos Colaboradores devem ser confidenciais, pessoais e intransferíveis. As senhas devem conter requisitos mínimos de segurança de acordo com as orientações da BRADO CAPITAL.

6.2. Utilização dos Ativos de Tecnologia da Informação

Os ativos de tecnologia da informação são recursos corporativos, de propriedade da BRADO CAPITAL, disponibilizados apenas para a execução das atividades funcionais

dos Colaboradores. É responsabilidade do Colaborador zelar pela proteção e pelas informações contidas nos ativos sob sua responsabilidade. Devem ser utilizados somente ativos homologados e autorizados pela BRADO CAPITAL.

7. Criptografia

O uso efetivo e adequado de um sistema de criptografia deve ser estabelecido com o intuito de assegurar a autenticidade, confidencialidade e integridade das informações.

8. Relacionamento com Terceiros

A proteção dos ativos acessados por Terceiros deve ser garantida, cabendo a cada uma das áreas envolvidas a responsabilidade por assegurar que os requisitos de segurança da informação sejam implementados e acordados com os Terceiros, para que se mitiguem os riscos associados aos acessos.

9. Auditoria e Conformidade

A BRADO CAPITAL deve auditar periodicamente as práticas de segurança da informação de forma a avaliar a conformidade das ações de seus Colaboradores em relação ao estabelecido nesta Política e na legislação aplicável.

10. Testes Periódicos De Segurança Para Os Sistemas De Informação

A BRADO CAPITAL assegura a realização de testes periódicos para os sistemas de informação, em especial para os mantidos em meio eletrônico.

10.1. Manutenção de Arquivos

A BRADO CAPITAL deve manter pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior, todos os documentos e informações exigidos pela Res. CVM 21/21, bem como toda a correspondência, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções, além de um arquivo segregado documentando as operações em

que tenha sido contraparte dos fundos de investimento ou das carteiras administradas. Os documentos informações podem ser guardados em meio físico ou eletrônico.

11. Monitoramento dos Sistemas de Comunicação

Os colaboradores devem ter ciência de que os e-mails enviados e recebidos, as ligações telefônicas e outros sistemas de informação são monitorados e gravados pela BRADO CAPITAL.

O Diretor de Compliance, no exercício de suas funções, realiza, no mínimo, [semestralmente] inspeções das comunicações eletrônicas e telefônicas, sobre uma amostragem significativa dos colaboradores, escolhida aleatoriamente, independentemente da suspeita ou ocorrência de quaisquer descumprimentos das regras estabelecidas nas normas da BRADO CAPITAL. O monitoramento realizado pelo Diretor de Compliance tem o propósito de verificar a aderência dos colaboradores às disposições estabelecidas nas normas da BRADO CAPITAL, e não representa uma invasão de privacidade.

Os registros obtidos pelo Diretor de Compliance através do monitoramento e gravação dos sistemas eletrônicos e telefônicos podem ser utilizados para detecção de violações dos normativos institucionais da BRADO CAPITAL, e servir como evidência em processos administrativos legais.

Existem sites, sistemas e diretórios que são de uso/acesso restrito na BRADO CAPITAL (apenas colaboradores específicos conseguem acessá-los). A tentativa de acessar sistemas, sites ou diretórios restritos por parte de um colaborador que não possui permissão para acessá-los é considerado falta grave.

O uso de telefone celular na BRADO CAPITAL só é permitido com autorização prévia do Diretor de *Compliance*.

12. Conflitos

Na existência de conflito entre os controles de segurança e uma necessidade de negócio específica, um novo cenário de controle deve ser analisado e implementado a fim de viabilizar os objetivos da BRADO CAPITAL, havendo ainda a necessidade de registro da aceitação dos riscos remanescentes por parte da diretoria.

13. Propriedade da Informação

Toda a informação produzida, enviada ou recebida pelos Colaboradores e Terceiros como resultado da atividade profissional, pertence à BRADO CAPITAL, o que inclui o conteúdo de todas as caixas de e-mails bem como todos os arquivos gravados nos diversos tipos de mídias. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

III. PROTEÇÃO DE DADOS PESSOAIS

1.1. Conceitos Gerais

- Anonimização - Processo utilizando os meios técnicos razoáveis e disponíveis na ocasião do Tratamento, para garantir que não seja possível associá-los, direta ou indireta, a uma pessoa natural.
- Dados Pessoais: É toda e qualquer informação relativa a uma pessoa física que direta ou indiretamente possa identificá-la. Por exemplo: nome, CPF, RG, telefone etc. Ressalta-se que a identificação indireta ocorre quando a pessoa é identificada após associação de um conjunto de dados pessoais (por exemplo, quando analisados, em conjunto, a idade, a geolocalização, a profissão e o gênero e o resultado da análise é a identificação de uma pessoa).
- Encarregado de Dados: É o encarregado dos dados nomeado pela BRADO CAPITAL que ficará responsável em atuar como canal de comunicação entre a BRADO CAPITAL, os Titulares dos Dados e os órgãos administrativos, judiciais e reguladores, em questões relacionadas à proteção de dados pessoais.

- Titular(es) de Dados: É toda a pessoa física a quem se referem os dados pessoais tratados. Sendo assim, incluem-se nesta definição todos os Colaboradores, os Terceiros, assim como os clientes pessoas físicas da BRADO CAPITAL e quaisquer pessoas físicas que tenham relacionamento com a BRADO CAPITAL.
- Tratamento - São os usos que a BRADO CAPITAL faz com os Dados Pessoais, seja ou não por meios automatizados, tais como coleta, produção, recepção, classificação, utilização, acesso, gravação, organização, estruturação, armazenamento, arquivamento, adaptação ou alteração, processamento, recuperação, consulta, utilização, divulgação por transmissão, difusão, extração, alinhamento ou combinação, restrição, eliminação, avaliação, ou destruição dos dados.

2. Responsabilidade dos Agentes de Tratamento

Nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – "LGPD"), são agentes de tratamento o Operador e o Controlador.

O Controlador é a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais (quando os dados serão tratados, de que forma serão tratados, quem estará envolvido nesse Tratamento, qual o período de Tratamento etc.). Enquanto o Operador é pessoa física ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador e mediante instruções deste, ficando obrigado a observar tais instruções, sob pena de responsabilização.

A seguir algumas hipóteses em que a BRADO CAPITAL atua como Controlador e/ou Operador:

- a) BRADO CAPITAL (Controladora) que contrata sistema de controle de informações de investidores (Operador) para armazenamento cadastral e controle do contato com o investidor. Nesse caso, a empresa que administra o sistema de

controle de informações seria o Operador pois está realizando o Tratamento dos Dados Pessoais dos Titulares a mando da BRADO CAPITAL; e

- b) BRADO CAPITAL (Controladora) que envia Dados Pessoais de seus empregados para escritório de contabilidade (Operador) para operações trabalhistas, tais como elaboração da folha de pagamento, controle de faltas, recolhimentos previdenciários etc.

Os agentes de tratamento de dados devem realizar o Tratamento de forma lícita e com a segurança que o Titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: (i) o modo pelo qual é realizado; (ii) o resultado e os riscos que razoavelmente dele se esperam; (iii) as técnicas de Tratamento de Dados Pessoais disponíveis à época em que foi realizado.

Nos termos da LGPD, a BRADO CAPITAL ou o Operador que, em razão do exercício de atividade de Tratamento de Dados Pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de Dados Pessoais, é obrigado a repará-lo, ressalvadas as exceções legais.

3. Direitos dos Titulares dos Dados Pessoais

| | |
|--|---|
| Confirmação e Acesso e confirmação da existência | Permite ao Titular a verificação do tratamento dos próprios Dados Pessoais e a verificação de quais os Dados Pessoais que a BRADO CAPITAL possui sobre ele. |
| Retificação e/ou atualização | Permite ao Titular que altere os Dados Pessoais incompletos, inexatos ou desatualizados. |
| Bloqueio, Anonimização ou Eliminação | Permite ao Titular solicitar o bloqueio dos próprios Dados Pessoais, suspendendo temporariamente ou a eliminação dos Dados Pessoais. |
| Portabilidade | Permite ao Titular solicitar a transferência de seus |

| | |
|---|--|
| | Dados Pessoais em formato estruturado para outra empresa. |
| Informação sobre o compartilhamento | Permite ao Titular saber quem são as entidades públicas e privadas com as quais a BRADO CAPITAL faz o uso compartilhado de Dados Pessoais. |
| Informação sobre a possibilidade de não consentir | O consentimento do Titular deve ser sempre livre e informado. |
| Revogação do consentimento e de oposição | O Titular tem o direito de retirar a permissão de uso de Dados Pessoais em relação às atividades que dependem do seu consentimento. |
| Reclamação | O Titular poderá realizar qualquer reclamação com relação aos próprios Dados Pessoais. |

4. Transferência Internacional de Dados

A Transferência Internacional de Dados Pessoais só poderá ser realizada para países que possuem leis de proteção de dados com nível de proteção aos dados equivalente ao da LGPD.

A transferência pode acontecer quando for necessária a cooperação entre órgãos públicos de inteligência de diferentes países para fins de investigação e processamento penal, ou quando a transferência for necessária para cumprimento de determinação legal ou regulatória pelo Controlador, quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato, para o exercício regular de direitos em processo judicial, administrativo ou arbitral ou para a execução de políticas públicas ou demandas legais do serviço público.

Além disso, a Transferência Internacional de Dados também poderá ocorrer quando o Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados previstos na LGPD, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos ou quando o Titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

IV. VIOLAÇÃO DA POLÍTICA

Os Colaboradores que descumprirem qualquer etapa do processo prevista nesta Política estarão sujeitos às sanções e/ou medidas disciplinares, rescisão contratual, podendo configurar responsabilidade nas esferas criminal, civil e administrativas aplicáveis, sem prejuízo da reparação de perdas e danos.

V. CONTROLE E REVISÃO

Esta Política será revisada anualmente pela equipe de [--] ou mediante a mudanças significativas no ambiente de negócio, responsabilidades, processos ou atividades. Serão utilizadas como base para sua atualização as legislações, instruções, regulamentações e autorregulamentações vigentes na data da sua revisão, e/ou as alterações nos procedimentos internos da BRADO CAPITAL.

VI. RESPONSABILIDADE PELA APROVAÇÃO

Esta Política foi elaborada pela Diretoria de [--] da BRADO CAPITAL.

VII. DISTRIBUIÇÃO DA POLÍTICA

Essa Política será distribuída eletronicamente (por e-mail e/ou pela intranet) para todos os colaboradores e Terceiros da BRADO CAPITAL.