Política de Segurança da Informação e Segurança Cibernética

BSI Capital Securitizadora S.A.

Agosto de 2022.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") entra em vigor em 25 de agosto de 2022 e será revisada anualmente de modo que sua alteração acontecerá caso seja constatada a necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

A última versão da Política, assim como demais materiais de suporte e políticas a ela relacionadas, estarão sempre disponíveis em seu website https://bsicapital.com.br/governanca/ para consulta de todos, em atenção ao compromisso de transparência assumido pela BSI Capital perante seus clientes e demais integrantes do mercado financeiro e de capitais.

Histórico das atualizações				
Versão	**Motivo da Alteração**	**Data**	**Departamento**	**Data da Aprovação**
1	Primeira Versão	25/08/2022	Compliance	25/08/2022

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURNAÇA CIBERNÉTICA

1. INTRODUÇÃO E OBJETIVO

A BSI Capital Securitizadora S.A. ("BSI Capital" ou "Securitizadora") é uma sociedade anônima registrada perante a Comissão de Valores Mobiliários ("CVM") na categoria de securitizadora e, assim, sujeita à sua regulamentação, em especial a Resolução CVM nº 60/21, bem como às previsões da Medida Provisória nº 1.103/2022.

Desse modo, em observância à legislação referida e à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), bem como em atenção à crescente necessidade de proteção dos sistemas de informação virtual em conformidade com as boas práticas do mercado, a BSI Capital elaborou e implementou a presente Política de Segurança da Informação e Segurança Cibernética.

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem como objetivo estabelecer e comunicar princípios, valores, conceitos, procedimentos, controles e diretrizes que assegurem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados nas atividades da BSI Capital, visando a redução da ocorrência de incidentes de segurança que afetem os seus negócios.

A partir da definição de ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, esta Política objetiva viabilizar a identificação de possíveis violações de segurança cibernética; mitigando, assim, os Riscos Cibernéticos e garantindo a continuidade dos negócios em caso de incidentes.

A Securitizadora dispõe de ambiente físico fechado, separado e de acesso restrito para alocar os equipamentos da rede com estações de trabalho individuais para cada Colaborador. A coordenação direta dos aspectos, procedimentos e atividades relativas à esta Política será feita pelo Diretor Compliance e PLD, em conjunto com os gestores diretos de cada sistema, sendo responsável pela realização de testes e treinamentos dos Colaboradores, conforme definido nesta Política.

Destaque-se que a presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio da BSI Capital, em especial a natureza das operações e a complexidade de suas atividades e processos; além de observar a sensibilidade dos dados e das informações sob responsabilidade da Securitizadora.

2. APLICABILIDADE

O disposto nesta Política deverá ser seguido e se aplica a todos os funcionários, diretores, acionistas, consultores, assessores, estagiários, parceiros comerciais, fornecedores e prestadores de serviço ("Colaboradores") que tenham relacionamento profissional com a BSI Capital, de modo a garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam destinados apenas ao cumprimento de suas atribuições.

É de responsabilidade de cada Colaborador todo prejuízo ou dano que vier a sofrer ou causar à BSI Capital ou a terceiros, em decorrência da não observância ao disposto nesta Política.

3. PRINCÍPIOS

Os ativos de informação figuram como os bens mais relevantes no mercado financeiro, uma vez que garantem a vantagem competitiva de seu detentor, sendo, portanto, imperioso tratá-los com responsabilidade. Por tais motivos, a BSI Capital sempre envidará os melhores esforços de modo a garantir a segurança dos dados sob sua custódia, assim como a qualidade e a continuidade dos serviços prestados.

Nesse sentido, as práticas implementadas serão norteadas sempre em conformidade com os princípios abaixo:

(i) Disponibilidade – garantir que as informações estejam acessíveis e disponíveis às pessoas previamente autorizadas;

(ii) Integridade – garantir que as informações sejam mantidas íntegras e que não sofram modificações indevidas (acidentais ou propositais);

(iii) Confidencialidade – garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

(iv) Acesso Controlado – garantir que o acesso às informações seja permanentemente restrito, monitorado e controlado, sendo revisto periodicamente e cancelado conforme a análise do caso concreto.

4. CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES

Os dados e informações tratados pela BSI Capital serão classificados consoante as categorias abaixo, tendo em vista a sua relevância:

i. Pública – documentos cuja informação foi aprovada pela diretoria para circulação pública (interna e externa), a exemplo de relatórios anuais, material para o site e correlatos;

ii. Interna - documentos cuja informação foi aprovada para circulação exclusivamente interna, a exemplo de memorandos internos, atas de reunião, relatórios de acompanhamento de emissões de valores mobiliários, entre outros;

iii. Confidencial – documentos cuja informação não pode ser disponibilizada em circulação externa, pois impactaria negativamente os negócios por questões estratégicas e de gestão;

iv. Sensível/Restrita – documentos cujas informações, internas ou confidenciais, são críticas ao desenvolvimento do negócio da BSI Capital, de modo que (a) são acobertadas por sigilo decorrente de lei, e (b) a sua perda e/ou indisponibilidade seriam prejudiciais à realização das atividades da BSI Capital, ao cumprimento de suas obrigações legais e à prestação adequada de seus serviços.

A BSI Capital compartilhará as informações sensíveis sempre que instada a fazê-lo em virtude de dispositivo legal, ato de autoridade competente, requerimento de entidade reguladora, e por determinação judicial.

5. GESTÃO E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

5.1. Regra Geral de Conduta

A BSI Capital, visando mitigar cada vez mais os riscos inerentes à utilização de seus sistemas, dados e informações, estabeleceu os procedimentos abaixo que deverão ser adotados por todos os Colaboradores:

- Informações Confidenciais somente deverão ser compartilhadas e disponibilizadas com demais Colaboradores que efetivamente necessitem ter conhecimento destas informações para desenvolvimento de suas atividades;

- É vedada a realização de cópias (físicas ou eletrônicas), bem como a impressão de documentos disponíveis na rede da Securitizadora, para circulação em ambiente externo à BSI Capital quando não destinados à condução dos negócios da Securitizadora;
- Os Colaboradores deverão atentar sempre para não deixar documentos, papeis e anotações que contenham Informação Confidencial sem supervisão em suas estações de trabalho ou em outro espaço físico da Securitizadora, em especial após o fim do expediente;
- É vedada a conexão de *pendrives*, *HD´*s externos e qualquer outro equipamento na rede da Securitizadora que não tenham sido previamente autorizados pela área de informática ou pelo gestor imediato do sistema;
- As impressões realizadas deverão ser imediatamente retiradas da estação da impressora para evitar a disponibilização indevida das informações ali contidas;
- É vedado o acesso a aplicativos de mensagem, sites, blogs, fotologs, *webmails*, redes sociais, grupos de redes sociais, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre raça, etnia, classe social, política, idade, sexo ou deficiência física), obsceno, pornográfico e ofensivo;
- A utilização dos ativos e sistemas disponibilizados pela Securitizadora, tais como computadores, internet, telefones, e-mail corporativo, entre outros, destina-se exclusivamente para desenvolvimento das atividades profissionais na condução dos negócios da BSI Capital. A sua utilização indevida para fins pessoais poderá acarretar penalidades diversas.

5.2. Controle de Acessos, Autenticação e Senha

Todo e qualquer acesso e uso dos sistemas de informação, bancos de dados, diretórios de rede e demais recursos será devidamente monitorado, controlado e restrito a menor permissão e privilégios possíveis.

Tais acessos e usos serão autorizados pelo gestor de cada sistema, devendo ser revistos de maneira periódica e cancelados tempestivamente ao término do contrato do Colaborador ou do Prestador de Serviços, podendo, ademais, serem revogados mediante solicitação do gestor do sistema ou de outro Colaborador dotado de poderes para tal.

O Colaborador é responsável por todos os atos executados com seu login e senha de acesso, uma vez que seu identificador é único e exclusivo, devendo seguir sempre as orientações contidas nesta Política, proibir o uso de seu equipamento por outras pessoas enquanto estiver logado e bloqueá-lo ao se ausentar.

A BSI Capital prioriza a conscientização e disseminação da cultura de segurança cibernética entre seus Colaboradores, de modo a (i) promover programas de capacitação e treinamentos periódicos direcionados aos seus Colaboradores, (ii) a circular memorandos internos para conscientização acerca de atualizações desta Política e de questões correlatas e (iii) a prestar informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

5.3. Acesso Remoto

A Securitizadora disponibiliza o acesso remoto aos seus Colaboradores mediante requisição prévia ao gestor do sistema, o qual avaliará e verificará a pertinência da solicitação do Colaborador caso a caso.

Aqueles Colaboradores que possuírem autorização para este tipo de acesso deverão (i) realizar o acesso remoto apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter *softwares* de proteção contra *malware*/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de Compliance e PLD qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Securitizadora e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

5.4. Prevenção contra Vírus, Arquivos e *Softwares* Maliciosos

A BSI Capital dispõe de controles de prevenção a vírus e outros *softwares* maliciosos providos por empresa qualificada e especializada no setor de tecnologia da informação, a qual foi contratada para realizar a manutenção preventiva e corretiva dos equipamentos (estações de trabalho e cabeamento) além de prestar suporte à rede e ao provedor de e-mails.

As dependências da BSI Capital também contam com equipamentos (serviços de *firewall*) necessários à proteção da sua rede interna contra ataques hackers e para estabelecimento de barreiras protetoras entre a internet e as informações arquivadas no seu servidor e nas estações de trabalho.

5.5. Cópias de Segurança (*Backup*)

A execução de procedimentos de *backup* é realizada de forma diária nos ativos de informação da BSI Capital, por meio do arquivamento de uma cópia de segurança no desktop ou notebook do Colaborador e em sistema de nuvem, visando a mitigação do risco de perda de dados ante à ocorrência de incidentes.

6. GESTÃO DE INCIDENTES

A BSI Capital possui controles de detecção de possíveis ataques cibernéticos em seu ambiente, tais como antivírus, AntiSpam, *firewall*, filtro de conteúdo, entre outros, a fim de evitar a ocorrência de incidentes. Contudo, no evento da sua ocorrência, os incidentes deverão ser imediatamente comunicados ao gestor imediato do sistema para que sejam adotadas as medidas definidas no Plano de Ação e de Resposta a Incidentes o mais breve possível.

Os incidentes serão classificados quanto à criticidade do seu impacto na continuidade do negócio da BSI Capital:

i. **Muito alta ou Crítica** - incidentes que expõem dados sensíveis da Securitizadora e de seus clientes capazes de comprometer a continuidade dos negócios;
ii. **Alta** - incidentes que possam interromper os serviços da BSI Capital ou de alguma maneira comprometer o adequado funcionamento de seus sistemas;
iii. **Moderada** - incidentes caracterizados por tentativas de acesso não autorizados aos sistemas da BSI Capital.
iv. **Baixa** - incidentes em hardwares ou softwares que sejam solucionados através de simples manutenção ou substituição.

Após a apuração da gravidade do incidente, o respectivo Plano de Ação e de Resposta será implementado.

7. CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios tem como escopo o reestabelecimento das operações a um nível aceitável, buscando minimizar impactos e perdas

de ativos da informação após um incidente de segurança cibernética por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

O supracitado processo deverá considerar, minimamente, os cenários relatados abaixo para a realização dos testes previstos na Política de Continuidade de Negócios:

i. Verificação de possíveis vulnerabilidades que possibilitem a cópia, o acesso e/ou a extração de dados sensíveis do sistema da BSI Capital;
ii. Execução de testes de intrusão à base de dados;
iii. Avaliação e estimativa do tempo de recuperação de acesso às informações de *backup* em hipótese de perda de dados sensíveis;
iv. Estratégias para a recuperação de informações sensíveis.

Todas as ocorrências devem ser registradas e avaliadas pela empresa de tecnologia da informação contratada pela BSI Capital para a determinação dos eventuais impactos causados nas operações.

8. MANUTENÇÃO DE ARQUIVOS

A Securitizadora manterá, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações dispostas nesta Política, bem como toda a documentação exigida pela Resolução CVM nº 60/21, incluindo, mas não se limitando a todos os papéis de trabalho, relatórios, testes e pareceres relacionados com o exercício das atividades da Securitizadora.

9. VIOLAÇÃO E PENALIDADES

Atividades suspeitas, incidentes e violações de segurança deverão ser informadas ao gestor imediato assim que a sua ocorrência for verificada, a fim de que as medidas necessárias sejam tomadas o mais breve possível.

Toda violação e/ou desvio às diretrizes desta Política será apurado para a determinação da sua extensão e posterior aplicação das sanções cabíveis aos envolvidos. O não cumprimento desta Política, intencional ou acidental, acarretará ações disciplinares e trabalhistas aos colaboradores da BSI Capital. Já os prestadores de serviços e parceiros de negócios estão sujeitos

à rescisão de seus contratos em que a BSI Capital é parte, bem como às penas de responsabilidade civil e criminal na extensão que a lei permitir.

10. CONSIDERAÇÕES FINAIS

A presente Política de Segurança da Informação e Segurança Cibernética deverá sempre ser analisada e compreendida em conjunto com as demais políticas internas da BSI Capital bem como em consonância com a legislação aplicável.

Em caso de dúvidas acerca das disposições desta Política e de suas aplicações, o Colaborador deverá consultar o Compliance por meio do e-mail: compliance@bsicapital.com.br ou através dos telefones (11) 4330-9780 e (11) 4330-9228. Não serão aceitas alegações de desconhecimento de seu conteúdo pelo Colaborador para fins de justificativa da prática de violação deste Código e das demais políticas internas da BSI Capital.