Sumário

1. Introdução

O **Grupo Presença**, em sua atuação estratégica como Securitizadora, gestora de fundos de investimento e provedora de serviços bancários (bancarizadora), lida diariamente com um volume expressivo e extremamente sensível de informações. A integridade, confidencialidade e disponibilidade desses dados, que incluem informações financeiras, estratégicas e, primordialmente, **dados pessoais** de clientes, cedentes, investidores, parceiros e colaboradores, são ativos críticos para a sustentabilidade, reputação e conformidade regulatória da organização.

Em um ambiente globalizado e crescentemente digital, as ameaças à segurança da informação evoluem constantemente, tornando imperativo um conjunto de diretrizes claras e um compromisso organizacional inabalável com a proteção desses ativos.

Esta **Política de Segurança da Informação (PSI)** estabelece o arcabouço fundamental e as diretrizes gerais para a proteção de todos os ativos de informação do Grupo Presença. Ela serve como base para a elaboração e aplicação de políticas mais específicas, como a **Política Cibernética** e a **Política de Cookies**, e está intrinsecamente alinhada à nossa **Política de Privacidade e Proteção de Dados**. Este documento reflete o compromisso do Grupo Presença em garantir que a segurança da informação seja um pilar estratégico integrado a todas as suas operações.

2. Objetivo

A presente Política de Segurança da Informação tem como objetivos primordiais e interligados:

- **Proteger os Ativos de Informação**: Assegurar a proteção de todos os ativos de informação do Grupo Presença contra ameaças internas e externas, intencionais ou acidentais, garantindo sua **confidencialidade, integridade e disponibilidade**.
- **Assegurar a Conformidade Legal e Regulatória**: Garantir o cumprimento rigoroso da legislação vigente, em especial a **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**, e das regulamentações específicas do setor financeiro e de capitais, como as emanadas pelo **Banco Central do Brasil (BACEN)**, **Comissão de Valores Mobiliários (CVM)** e **Conselho Monetário Nacional (CMN)**, incluindo, mas não se limitando, às **Resoluções CMN nº 4.893/2021** e **Resolução BCB n° 197/2022** (e suas sucessoras).
- **Minimizar Riscos**: Reduzir a probabilidade de ocorrência de incidentes de segurança da informação e seus potenciais impactos, através da identificação, avaliação e tratamento proativo de riscos.
- **Estabelecer Responsabilidades**: Definir papéis e responsabilidades claros para todos os colaboradores, parceiros e terceiros em relação à segurança da informação.
- **Fomentar a Conscientização**: Promover uma cultura de segurança da informação, conscientizando e capacitando toda a equipe sobre as melhores práticas e a importância da proteção dos dados.
- **Apoiar a Continuidade dos Negócios**: Garantir que as operações do Grupo Presença possam continuar, ou ser prontamente restauradas, em caso de eventos adversos, minimizando interrupções e perdas.
- **Preservar a Reputação**: Proteger a imagem e a reputação do Grupo Presença, consolidando a confiança de seus clientes, investidores e demais stakeholders.

3. Abrangência

Esta Política de Segurança da Informação aplica-se a:

- **Todos os colaboradores do Grupo Presença**, independentemente do nível hierárquico, modalidade de contratação ou localização (presencial ou remota).
- **Terceiros, prestadores de serviços, parceiros comerciais, consultores e quaisquer agentes externos** que tenham acesso, processem ou armazenem informações do Grupo Presença ou em seu nome.
- **Todos os ativos de informação** do Grupo Presença, incluindo, mas não se limitando a: dados eletrônicos e físicos, sistemas, softwares, hardware, redes, serviços em nuvem, bancos de dados, documentos, contratos e mídias de armazenamento, onde quer que estejam localizados ou armazenados.
- **Todas as operações e processos de negócio** do Grupo Presença, abrangendo as atividades de securitização, gestão de fundos de investimento e operações bancárias.

4. Principais Conceitos

Para o entendimento desta Política, são adotados os seguintes conceitos, que complementam os definidos na *Política de Privacidade e Proteção de Dados* e *Política Cibernética* do Grupo Presença:

- **Ativo de Informação**: Qualquer informação ou sistema de informação que tenha valor para o Grupo Presença. Isso inclui hardware, software, dados (pessoais ou não), documentos, serviços, pessoas e instalações.

- **Ameaça**: Potencial causa de um incidente indesejado, que pode resultar em dano a um sistema ou organização. Ex: malware, erro humano, ataque cibernético.
- **Vulnerabilidade**: Fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças. Ex: software desatualizado, senha fraca.
- **Risco**: Combinação da probabilidade de ocorrência de uma ameaça e do impacto resultante para o Grupo Presença.
- **Confidencialidade**: Propriedade que garante que a informação não esteja disponível ou seja divulgada a indivíduos, entidades ou processos não autorizados.
- **Integridade**: Propriedade que garante que a informação seja completa e precisa, e que não foi modificada de maneira não autorizada.
- **Disponibilidade**: Propriedade que garante que a informação e os sistemas associados estejam acessíveis e utilizáveis por uma entidade autorizada quando necessário.
- **Dados Pessoais**: Conforme definido na LGPD, qualquer informação relacionada a pessoa natural identificada ou identificável.
- **Dados Pessoais Sensíveis**: Conforme definido na LGPD, dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **DPO (Data Protection Officer) / Encarregado de Dados**: Pessoa física ou jurídica designada para atuar como canal de comunicação entre o Grupo Presença, os titulares dos dados e a ANPD, conforme detalhado na *Política de Privacidade e Proteção de Dados*.

5. Princípios Fundamentais da Segurança da Informação

O Grupo Presença adota os seguintes princípios para guiar todas as ações e decisões relacionadas à segurança da informação:

- **Legalidade e Conformidade Regulatória**: Todas as atividades de segurança da informação devem estar em conformidade com as leis, regulamentos e normas aplicáveis, incluindo LGPD, e as regulamentações setoriais (BACEN, CVM, CMN).
- **Responsabilidade**: A segurança da informação é responsabilidade de todos que acessam ou utilizam os ativos do Grupo Presença, com responsabilidades específicas definidas para a alta direção, gestores, DPO e equipe de TI.
- **Minimização de Privilégios (Necessidade)**: O acesso aos ativos de informação deve ser concedido apenas na medida estritamente necessária para o desempenho das funções do colaborador ou terceiro ("need-to-know" e "least privilege").
- **Transparência**: As práticas de segurança da informação devem ser claras e compreensíveis, especialmente no que tange ao tratamento de dados pessoais, garantindo que os titulares estejam cientes de como suas informações são protegidas.
- **Prevenção**: Priorizar a implementação de medidas proativas para prevenir incidentes de segurança, em vez de apenas reagir a eles.
- **Detecção e Resposta**: Desenvolver capacidades para detectar incidentes de segurança rapidamente e responder a eles de forma eficaz, mitigando danos e garantindo a continuidade das operações.
- **Melhoria Contínua**: A segurança da informação deve ser um processo contínuo de avaliação, aprimoramento e adaptação às novas ameaças e tecnologias.
- **Segurança por Design e por Padrão**: A segurança deve ser considerada desde a concepção de novos sistemas, processos e serviços, e as

configurações de segurança padrão devem ser as mais restritivas possíveis.

6. Diretrizes de Segurança da Informação

Esta seção detalha as diretrizes de segurança da informação aplicáveis a todo o Grupo Presença:

6.1. Ativos de Informação

- **Inventário e Catalogação**: Manter um inventário completo e atualizado de todos os ativos de informação, identificando seu proprietário, localização, valor e criticidade.
- **Propriedade e Responsabilidade**: Designar um proprietário para cada ativo de informação, responsável pela sua segurança e pelo cumprimento das políticas relacionadas.
- **Descarte Seguro**: Estabelecer e seguir procedimentos rigorosos para o descarte seguro de informações e ativos, garantindo que dados confidenciais não sejam recuperáveis.

6.2. Classificação da Informação

Todas as informações geradas, processadas ou armazenadas pelo Grupo Presença devem ser classificadas de acordo com seu nível de sensibilidade e valor, visando aplicar os controles de segurança adequados. A classificação deve considerar o impacto potencial de sua divulgação, alteração ou destruição não autorizada.

- **Níveis de Classificação**:
  - **Pública**: Informações que podem ser divulgadas a qualquer pessoa sem restrições.

- **Interna**: Informações que, embora não confidenciais, são de uso exclusivo do Grupo Presença e sua divulgação externa não autorizada pode gerar algum tipo de desconforto ou desvantagem.
- **Confidencial**: Informações cujo acesso não autorizado, divulgação, alteração ou destruição poderia causar dano significativo ao Grupo Presença ou aos titulares dos dados. Inclui, mas não se limita a, **dados pessoais e dados financeiros** (ex: estratégias de negócio, dados de clientes, dados de securitização).
- **Restrita (Dados Pessoais Sensíveis)**: Categoria mais alta, destinada a informações cuja divulgação ou uso indevido causaria dano severo e irrecuperável ao Grupo Presença ou aos titulares dos dados. Inclui **dados pessoais sensíveis** conforme LGPD, dados de autenticação de alto privilégio, etc.

- **Rotulagem e Manuseio**: As informações devem ser rotuladas de acordo com sua classificação e manuseadas de forma consistente com os requisitos de segurança definidos para cada nível.

6.3. Controles de Acesso

O acesso aos ativos de informação do Grupo Presença deve ser rigorosamente controlado e baseado no princípio do mínimo privilégio.

- **Acesso Lógico**: Implementar e gerenciar controles de acesso lógico (usuário e senha, autenticação multifator - MFA) a sistemas, redes e dados. Senhas devem ser robustas e trocadas periodicamente.
- **Acesso Físico**: Controlar o acesso físico às instalações, áreas seguras (data centers, salas de servidores) e equipamentos que contenham ativos de informação sensíveis.

- **Revisão de Acessos**: Realizar revisões periódicas das permissões de acesso, garantindo que estejam sempre atualizadas e em conformidade com as funções dos usuários.
- **Controle de Acesso Remoto**: O acesso remoto deve ser protegido por VPN (Virtual Private Network) e MFA.

6.4. Segurança da Infraestrutura e Redes

- **Proteção de Perímetro**: Implementar firewalls e sistemas de prevenção e detecção de intrusões (IPS/IDS) para proteger a rede contra acessos não autorizados e ataques.
- **Segmentação de Rede**: Dividir a rede em segmentos lógicos para isolar informações críticas e dados pessoais, limitando o impacto de possíveis incidentes.
- **Monitoramento**: Monitorar ativamente o tráfego de rede e os logs de segurança para detectar atividades suspeitas e responder a elas prontamente.

6.5. Proteção contra Malwares e Ameaças Digitais

- **Antimalware**: Instalar e manter softwares antimalware atualizados em todos os dispositivos (estações de trabalho, servidores, dispositivos móveis) que acessem os ativos do Grupo Presença.
- **Controles de Navegação**: Utilizar soluções que filtrem conteúdo malicioso da internet e bloqueiem acessos a sites não confiáveis.
- **Atualização de Sistemas**: Manter sistemas operacionais, aplicações e softwares sempre atualizados com os últimos patches de segurança.

6.6. Criptografia e Pseudonimização

- **Uso de Criptografia**: Implementar criptografia para proteger dados sensíveis, especialmente dados pessoais, tanto em trânsito (comunicações) quanto em repouso (armazenamento em discos, bancos de dados).
- **Gerenciamento de Chaves**: Estabelecer um processo seguro para geração, armazenamento e gerenciamento de chaves criptográficas.
- **Pseudonimização e Anonimização**: Onde aplicável e viável, utilizar técnicas de pseudonimização e anonimização de dados para reduzir o risco de identificação de titulares, em conformidade com a LGPD e a *Politica de Privacidade e Proteção de Dados*.

6.7. Desenvolvimento e Aquisição Segura de Sistemas

- **Segurança por Design**: Exigir que a segurança seja incorporada desde as fases iniciais de projeto e desenvolvimento de novos sistemas e aplicações (Security by Design).
- **Teste de Segurança**: Realizar testes de segurança (testes de penetração, análise de código) em sistemas antes de sua implementação em produção.
- **Cláusulas Contratuais**: Incluir requisitos de segurança da informação em todos os contratos de aquisição de software e serviços de desenvolvimento.

6.8. Gestão de Vulnerabilidades e Patches

- **Varreduras de Vulnerabilidade**: Realizar varreduras periódicas de vulnerabilidade em sistemas e aplicações para identificar e corrigir falhas de segurança.
- **Gestão de Patches**: Implementar um processo formal para avaliação, teste e aplicação de patches de segurança em tempo hábil.

6.9. Backups e Recuperação de Desastres

- **Política de Backup**: Manter uma política de backup robusta para todos os dados críticos, incluindo dados pessoais, com rotinas definidas de frequência, tipo de backup e período de retenção.
- **Testes de Restauração**: Realizar testes periódicos de restauração de dados para garantir a eficácia dos backups e a capacidade de recuperação em caso de perda.
- **Planos de Recuperação de Desastres (DRP)**: Desenvolver, documentar e testar planos de recuperação de desastres para garantir a continuidade das operações em caso de incidentes maiores, conforme detalhado na *Política Cibernética*.

6.10. Segurança Física e Ambiental

- **Controle de Acesso Físico**: Restringir o acesso físico a áreas sensíveis (salas de servidores, arquivos confidenciais) através de controles apropriados (cartões de acesso, biometria).
- **Proteção Ambiental**: Implementar medidas de proteção contra incêndios, inundações, falhas de energia e outras ameaças ambientais que possam comprometer a segurança dos ativos.

6.11. Segurança para Dispositivos Móveis e Teletrabalho

- **Política de Dispositivos Móveis**: Estabelecer diretrizes claras para o uso seguro de dispositivos móveis (smartphones, tablets, notebooks) que acessam informações do Grupo Presença.
- **Acesso Remoto Seguro**: Garantir que o teletrabalho e o acesso remoto sejam realizados através de conexões seguras (VPN), com dispositivos protegidos e conformes às políticas internas.

- **Proteção de Dados em Dispositivos**: Implementar criptografia de disco, bloqueio de tela e funcionalidades de limpeza remota para dispositivos móveis que armazenem dados corporativos.

6.12. Uso de Serviços de Terceiros (incluindo Cloud Computing).

- **Due Diligence**: Antes de contratar qualquer serviço de terceiro que envolva o tratamento ou armazenamento de ativos de informação do Grupo Presença (especialmente dados pessoais), realizar uma avaliação rigorosa de segurança e conformidade do fornecedor.
- **Contratos e Acordos**: Assegurar que os contratos com terceiros incluam cláusulas claras sobre segurança da informação, proteção de dados (LGPD), responsabilidades, medidas de segurança exigidas, direitos de auditoria e procedimentos para tratamento de incidentes, em conformidade com a **Resolução CMN nº 4.893/2021** e a *Política de Privacidade e Proteção de Dados*.
- **Monitoramento Contínuo**: Monitorar e auditar periodicamente os provedores de serviços para garantir a manutenção dos níveis de segurança e conformidade.

6.13. Gestão de Incidentes de Segurança da Informação

- **Plano de Resposta**: Manter um Plano de Resposta a Incidentes (IRP) detalhado e testado, que defina os procedimentos para detecção, análise, contenção, erradicação, recuperação e análise pós-incidente, conforme detalhado na *Política Cibernética*.
- **Comunicação**: Estabelecer procedimentos para a comunicação de incidentes de segurança da informação aos stakeholders internos e externos, incluindo a notificação à ANPD e aos titulares dos dados afetados, conforme os requisitos da LGPD.

- **Lições Aprendidas**: Realizar análises pós-incidente para identificar as causas raiz e implementar ações corretivas para evitar reincidências.

6.14. Conscientização, Treinamento e Cultura de Segurança

- **Programa Contínuo**: Implementar um programa contínuo e obrigatório de conscientização e treinamento em segurança da informação para todos os colaboradores e terceiros com acesso aos ativos do Grupo Presença.
- **Cultura de Segurança**: Promover uma cultura onde a segurança da informação é uma responsabilidade compartilhada por todos e um valor fundamental da organização, incentivando a denúncia proativa de vulnerabilidades e atividades suspeitas.

7. Funções e Responsabilidades

A segurança da informação é uma responsabilidade coletiva, com atribuições específicas para cada nível e função dentro do Grupo Presença:

- **Alta Direção (CEO e Conselhos)**: Responsável por aprovar esta Política, fornecer os recursos necessários para sua implementação e garantir que a segurança da informação seja prioridade estratégica.
- **DPO (Encarregado de Dados)**: Conforme *Política de Privacidade e Proteção de Dados*, atua como consultor para LGPD, ponto de contato com titulares e ANPD, e monitora a conformidade das operações com dados pessoais.
- **Departamento de Tecnologia da Informação (TI)**: Responsável pela implementação, manutenção e monitoramento dos controles técnicos de segurança, gestão da infraestrutura, sistemas, redes e pela resposta técnica a incidentes.

- **Departamento de Compliance**: Assegura que as políticas de segurança da informação estejam alinhadas às leis e regulamentações, participa da gestão de riscos e incidentes e promove a cultura de conformidade.
- **Gerentes e Líderes de Equipe**: Responsáveis por garantir que suas equipes compreendam e cumpram esta Política, promovendo a segurança da informação em suas respectivas áreas.
- **Todos os Colaboradores e Terceiros**: Responsáveis por compreender e cumprir esta Política, bem como todas as normas e procedimentos de segurança da informação relacionados, e por reportar qualquer incidente ou preocupação.

8. Gestão de Riscos de Segurança da Informação

O Grupo Presença adota uma abordagem baseada em riscos para a gestão da segurança da informação.

- **Metodologia de Análise de Riscos**: Utilizar uma metodologia formal para identificar, analisar, avaliar e tratar os riscos de segurança da informação, considerando as ameaças e vulnerabilidades aos ativos.
- **Avaliação Contínua**: Realizar avaliações de risco periódicas e sempre que houver mudanças significativas no ambiente (novos sistemas, processos ou regulamentações).
- **Plano de Tratamento de Riscos**: Desenvolver e implementar planos de tratamento para mitigar, transferir, aceitar ou evitar os riscos identificados.

9. Legislação e Regulamentação Aplicável

Esta Política de Segurança da Informação é concebida e deve ser interpretada e executada em total conformidade com as seguintes leis e regulamentações brasileiras e setoriais:

- **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**: Estabelece as regras para o tratamento de dados pessoais.
- **Resolução CMN nº 4.893, de 25 de fevereiro de 2021 (e suas sucessoras)**: Dispõe sobre os requisitos para a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução BCB n° 197, de 11 de março de 2022 (e suas sucessoras)**: Consolida os requisitos da política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados por determinadas instituições reguladas pelo BCB.
- **Circular CVM nº 617, de 22 de dezembro de 2020 (e suas sucessoras)**: Dispõe sobre a constituição, o funcionamento e a administração de fundos de investimento, bem como sobre a prestação de serviços para os fundos. Inclui requisitos de segurança e controles internos.
- **Legislação Específica para Securitizadora**: Regulamentação de emissão e registro de Certificados de Recebíveis Imobiliários (CRIs) e Certificados de Recebíveis do Agronegócio (CRAs) e outras operações.
- **Marco Civil da Internet (Lei nº 12.965/2014)**: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- **Código Penal Brasileiro**: Artigos relacionados a crimes informáticos.
- **Outras normas e regulamentações** emitidas pelo Banco Central do Brasil (BACEN), Comissão de Valores Mobiliários (CVM) e Conselho Monetário Nacional (CMN) aplicáveis às atividades do Grupo Presença.

O Grupo Presença manterá um monitoramento constante das alterações nestas legislações e regulamentações, garantindo a atualização contínua desta Política e de seus processos internos.

10. Conformidade e Auditoria

- **Monitoramento Contínuo**: Monitorar ativamente o cumprimento desta Política e de seus procedimentos relacionados.
- **Auditorias Internas e Externas**: Realizar auditorias periódicas, internas e externas, para avaliar a eficácia dos controles de segurança da informação e a conformidade com esta Política e a legislação aplicável.
- **Relatórios de Conformidade**: Gerar relatórios de conformidade para a alta direção e, quando exigido, para os órgãos reguladores.

11. Disposições Finais

O descumprimento desta Política de Segurança da Informação, bem como das demais normas e procedimentos de segurança, poderá acarretar sanções disciplinares, cíveis e/ou criminais, de acordo com a gravidade da infração, a legislação vigente e as políticas internas do Grupo Presença.

O Grupo Presença se reserva o direito de modificar o conteúdo desta Política a qualquer momento, conforme exigências legais, regulatórias, novas tecnologias ou necessidades internas. A versão mais recente será disponibilizada em seus canais de comunicação internos e website oficial, com a indicação da data de sua última atualização.

12. Vigência e Revisão

Esta Política de Segurança da Informação entra em vigor a partir de **03 /10 /2025**.

Será revisada anualmente ou sempre que houver mudanças significativas na legislação, regulamentação, tecnologia, estrutura organizacional ou nos processos internos do Grupo Presença, garantindo sua contínua adequação e eficácia.

13. Aprovação

Esta Política de Segurança da Informação foi formalmente aprovada pela Alta Administração e lideranças técnicas do Grupo Presença, atestando o compromisso da organização com a segurança de seus ativos de informação e a proteção dos dados