Sumário

1. Introdução

O **Grupo Presença**, atuando como Securitizadora, gestora de fundos de investimento e provedora de serviços bancários (Bancarizadora), reconhece a criticidade e a extrema sensibilidade dos dados e informações que processa diariamente. Em especial, os **dados pessoais e financeiros** de seus clientes, cedentes, investidores, parceiros comerciais, colaboradores e demais stakeholders representam ativos de valor inestimável, cuja proteção é vital.

Em um cenário digital em constante evolução, marcado por crescentes desafios e ameaças cibernéticas, a segurança desses ativos é fundamental não apenas para a sustentabilidade e a reputação de nossos negócios, mas, acima de tudo, para garantir a **confiança** e o **cumprimento rigoroso** de nossas responsabilidades legais e regulatórias.

Esta **Política de Segurança Cibernética** emerge como um pilar essencial, complementando e aprofundando o compromisso já estabelecido em nossa *Política de Privacidade e Proteção de Dados*. Ela detalha as diretrizes e os requisitos mandatórios para a proteção de nossos sistemas, redes, infraestrutura e todos os dados contra ameaças digitais, reforçando a diligência do Grupo Presença em resguardar as informações com base nos pilares de confidencialidade, integridade e disponibilidade.

2. Objetivo

A presente Política de Segurança Cibernética tem como objetivos primordiais:

- **Estabelecer diretrizes e responsabilidades claras** para o gerenciamento eficaz da segurança da informação cibernética em todas as operações, processos e tecnologias utilizadas pelo Grupo Presença.
- **Prevenir, identificar e mitigar** proativamente vulnerabilidades e incidentes cibernéticos que possam comprometer a segurança de nossos ativos digitais e informações, incluindo, mas não se limitando a, dados pessoais, dados financeiros, informações estratégicas e propriedade intelectual.
- **Assegurar a confidencialidade, integridade e disponibilidade** de todas as informações sob nossa responsabilidade, por meio da implementação e manutenção de controles técnicos, organizacionais e

procedimentais robustos, adaptados às melhores práticas de segurança da informação.

- **Garantir a estrita conformidade** com a legislação vigente, notadamente a **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)** –, bem como com as circulares, normas, resoluções e regulamentações específicas e atualizadas emitidas por órgãos reguladores da maior relevância para nosso setor, tais como o **Banco Central do Brasil (BACEN)**, a **Comissão de Valores Mobiliários (CVM)** e, em particular, a **Resolução CMN nº 4.893/2021** (e suas sucessoras), que aborda requisitos para contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, e demais normativos aplicáveis ao mercado financeiro e de capitais.
- **Fomentar a melhoria contínua** dos procedimentos de segurança, a revisão constante dos riscos e a promoção de uma cultura de conscientização em segurança cibernética em todos os níveis da organização, reforçando a confiança de todos os stakeholders do Grupo Presença.

3. Principais Conceitos de Segurança Cibernética

A Segurança Cibernética, no contexto do **Grupo Presença**, é a prática de proteger sistemas, redes e programas contra ataques digitais. Seu fundamento reside na preservação das informações a que temos acesso, com ênfase na proteção dos dados pessoais, assegurando seus pilares essenciais:

- **Confidencialidade**: Garante que apenas indivíduos ou sistemas devidamente autorizados e com base legal possam acessar informações sensíveis, especialmente **dados pessoais e dados pessoais sensíveis**. Evita a exposição de dados a pessoas não autorizadas por meio de mecanismos como criptografia robusta, autenticação multifator e controle de acesso baseado no princípio do mínimo privilégio, assegurando que as informações permaneçam privadas e protegidas contra acesso indevido ou espionagem, alinhado ao *princípio da Segurança da LGPD*.
- **Integridade**: Assegura a precisão, completude e consistência das informações, garantindo que os dados não sejam alterados de forma não autorizada, acidental ou maliciosa. Implementamos métodos de processamento que mantêm a validade e exatidão dos dados, o que se

alinha ao *princípio da Qualidade dos Dados da LGPD*, exigindo que os dados tratados sejam claros, exatos, relevantes e atualizados.

- **Disponibilidade**: Garante que os usuários autorizados tenham acesso contínuo e confiável às informações e aos sistemas que processam **dados pessoais**, sempre que necessário. Evita interrupções sistêmicas ou operacionais significativas que possam acarretar prejuízo financeiro, operacional ou impedir o exercício dos direitos dos titulares dos dados.
- **Risco Cibernéticos**: Entende-se como a probabilidade de ocorrência de ataques cibernéticos (internos ou externos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede, sabotagem, violação de acessos e privacidade) e o impacto potencial que podem causar. A materialização desses riscos pode expor **dados pessoais**, redes e sistemas do Grupo Presença, gerando danos financeiros, reputacionais e, crucialmente, incidentes de segurança de dados pessoais com implicações legais e regulatórias severas sob a LGPD.

4. O Papel do Encarregado de Dados (DPO) no Grupo Presença

O Encarregado de Dados (DPO - Data Protection Officer), conforme estabelecido na *Política de Privacidade dos Dados - Grupo Presença, Seção 4: Conceitos Fundamentais*, é a pessoa física ou jurídica designada pelo **Grupo Presença** para ser o canal de comunicação entre a empresa (Controladora), os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD). Sua atuação é fundamental para a conformidade e a segurança cibernética, especialmente no que tange aos dados pessoais.

As principais responsabilidades do DPO incluem:

- **Orientação e Aconselhamento**: Oferecer consultoria e orientação estratégica à alta administração, colaboradores e equipes sobre as obrigações da LGPD, as regulamentações setoriais (BACEN, CVM) e as melhores práticas de proteção de dados e segurança cibernética.
- **Ponto de Contato Central**: Atuar como o principal interlocutor do Grupo Presença junto aos Titulares de Dados para o exercício de seus direitos (acesso, correção, eliminação, portabilidade, etc.), conforme *Política de Privacidade dos Dados - Grupo Presença, Seção 14: Direitos dos Titulares*. Também é o contato primário com a ANPD para fiscalizações, auditorias e comunicação de incidentes.

- **Monitoramento da Conformidade**: Supervisionar a implementação e o cumprimento das políticas internas de proteção de dados e segurança da informação, incluindo esta Política Cibernética, através de auditorias internas e avaliação de processos.
- **Gestão de Incidentes de Segurança com Dados Pessoais**: Coordenar a resposta a incidentes de segurança que envolvam dados pessoais, garantindo que a notificação à ANPD e aos titulares ocorra nos prazos e termos exigidos pela LGPD, conforme detalhado na *Politica de Privacidade dos Dados - Grupo Presença, Seção 15: Ações Internas do Grupo Presença para Proteção de Dados*.
- **Treinamento e Conscientização**: Promover e acompanhar programas de treinamento contínuo para todos os colaboradores, garantindo que estejam atualizados sobre as práticas de segurança e as obrigações legais, conforme *Política de Privacidade dos Dados - Grupo Presença, Seção 15: Ações Internas do Grupo Presença para Proteção de Dados*.

5. Gestão de Segurança Cibernética e da Informação

O **Grupo Presença** adota políticas e normas rigorosas para assegurar que as informações, em particular os dados pessoais, sejam protegidas de forma abrangente. Isso é feito em conformidade com as exigências dos Órgãos reguladores (BACEN, CVM, ANPD) e por meio da aplicação das melhores práticas de mercado. As principais diretrizes são:

5.1. Gestão de Ativos da Informação

Todos os ativos de informação, que incluem sistemas, softwares, bancos de dados, equipamentos e mídias que armazenam ou processam **dados pessoais**, devem ser inventariados de forma individual e detalhada.

- **Inventário Detalhado**: Manter um registro atualizado de todos os ativos, indicando sua localização, proprietário, finalidade e a presença de dados pessoais.
- **Ciclo de Vida do Ativo**: Gerenciar o ciclo de vida completo de cada ativo, desde a aquisição, uso, manutenção até o descarte seguro, garantindo que os dados pessoais sejam tratados adequadamente em todas as fases.

- **Avaliação Periódica**: Realizar auditorias regulares para verificar a precisão do inventário e a conformidade das configurações de segurança dos ativos.

5.2. Classificação da Informação

Todas as informações devem ser classificadas de acordo com seu grau de confidencialidade e a proteção necessária, incluindo, quando aplicável, o uso de criptografia. A classificação considerará a natureza dos dados, com especial atenção aos dados pessoais e dados pessoais sensíveis, categorizando-as em:

- **Restrita**: Informações de uso interno, limitadas a um grupo específico de colaboradores.
- **Confidencial**: Informações sigilosas que não podem ser divulgadas publicamente, incluindo **todos os dados pessoais e dados pessoais sensíveis**. Exige os mais altos níveis de segurança e controle de acesso.
- **Pública**: Informações de conhecimento geral, sem restrições de divulgação.
- **Diretrizes e Treinamento**: Desenvolver um guia claro para classificação e treinar todos os colaboradores para aplicá-la corretamente.
- **Controles Baseados na Classificação**: Implementar controles de acesso e proteção (ex: criptografia, Data Loss Prevention – DLP) que variem conforme a classificação da informação.

5.3. Gestão de Acessos

A cessão, revisão ou exclusão de acessos a sistemas e informações deve ser rigorosamente controlada, baseada nos princípios de autoridade, autenticidade e **privilégios mínimos**, garantindo que os colaboradores e parceiros acessem apenas o que é estritamente necessário para suas funções.

- **Controle de Acesso Baseado em Papéis (RBAC)**: Definir e aplicar papéis e permissões claros para cada função na empresa, limitando o acesso a sistemas e dados aos usuários autorizados.
- **Autenticação Forte**: Exigir autenticação multifator (MFA) para acesso a sistemas críticos e dados sensíveis.
- **Revisões Periódicas**: Realizar revisões regulares e documentadas dos acessos concedidos para garantir sua contínua adequação e remover

permissões desnecessárias. Acessos de ex-colaboradores devem ser revogados imediatamente.

- **Rastreabilidade**: Manter logs detalhados de todos os acessos, permitindo a rastreabilidade e auditoria em caso de necessidade.

5.4. Gestão de Riscos

Qualquer risco cibernético deve ser mapeado e gerido proativamente. Implementamos uma metodologia formal para identificar, analisar, avaliar e tratar riscos, com foco nos riscos à privacidade dos dados pessoais.

- **Análise de Vulnerabilidade e Ameaças**: Realizar análises contínuas para identificar vulnerabilidades em sistemas e processos, e avaliar as ameaças potenciais.
- **DPIA (Data Protection Impact Assessment)**: Conduzir Avaliações de Impacto à Proteção de Dados (DPIA) para novos projetos, tecnologias ou operações que possam apresentar alto risco à privacidade dos titulares, conforme estabelecido na *Política de Privacidade dos Dados - Grupo Presença, Seção 15: Ações Internas do Grupo Presença para Proteção de Dados*.
- **Registro de Riscos**: Manter um registro atualizado de todos os riscos identificados, incluindo sua avaliação, medidas de mitigação e responsáveis pelo acompanhamento.
- **Testes de Invasão (Pentests)**: Realizar testes de penetração e varreduras de vulnerabilidade periódicas por empresas especializadas.

5.5. Gestão da Continuidade de Negócios

O gerenciamento de riscos inclui um sistema de manutenção robusto para garantir a continuidade das operações do Grupo Presença.

- **Planos de Continuidade de Negócios (BCP) e Recuperação de Desastres (DRP)**: Desenvolver e documentar planos abrangentes que prevejam a rápida recuperação dos sistemas e dados, especialmente aqueles que processam dados pessoais, em cenários de falhas de TI, ciberataques ou desastres.
- **Testes e Simulações**: Testar e revisar regularmente os planos para garantir sua eficácia e a prontidão da equipe em cenários de crise.

- **Comunicação de Crise**: Incluir um plano de comunicação para informar stakeholders (clientes, reguladores, imprensa) em caso de interrupção significativa.

5.6. Gestão de Incidentes de Segurança

Qualquer incidente que envolva segurança cibernética deve ser tratado de forma estruturada, com foco na proteção das informações e dos dados pessoais.

- **Plano de Resposta a Incidentes (IRP)**: Manter um IRP bem definido e testado, que detalhe as etapas desde a detecção até a recuperação e análise pós-incidente, incluindo a equipe de resposta e suas responsabilidades. Este plano é coordenado com as diretrizes do *Plano de Resposta a Incidentes* descrito na *Política de Privacidade dos Dados - Grupo Presença, Seção 15*.
- **Canais de Denúncia**: Estabelecer canais claros e acessíveis para que colaboradores e terceiros possam reportar suspeitas de incidentes de segurança.
- **Ferramentas de Detecção e Monitoramento**: Utilizar ferramentas de Security Information and Event Management (SIEM) e outras soluções para monitorar eventos de segurança e detectar anomalias em tempo real.
- **Coordenação com o DPO**: O DPO será imediatamente acionado em caso de incidentes envolvendo dados pessoais para avaliar impactos, coordenar a resposta e determinar a necessidade de comunicação à ANPD e aos titulares, conforme exigido pela LGPD.

5.7. Conscientização e Treinamento em Segurança Cibernética

O **Grupo Presença** garante a divulgação contínua dos princípios e diretrizes de Segurança Cibernética.

- **Programa de Treinamento Obrigatório**: Implementar um programa de treinamento anual e obrigatório para todos os colaboradores e prestadores de serviços, abordando segurança da informação, proteção de dados (LGPD) e as políticas internas.
- **Conteúdo Engajador**: Utilizar módulos de e-learning, vídeos, quizzes e campanhas internas para reforçar o tema e manter a equipe engajada.

- **Simulações**: Realizar simulações de ataques (ex: phishing) para testar a resiliência humana e reforçar a educação.
- **Cultura de Segurança**: Promover uma cultura onde a segurança cibernética e a proteção de dados são responsabilidades compartilhadas por todos, incentivando a comunicação proativa de riscos e vulnerabilidades.

6. Processamento, Armazenamento de Dados e Computação em Nuvem

Ao utilizar serviços externos, especialmente em nuvem, que envolvam o processamento ou armazenamento de **dados pessoais**, o **Grupo Presença** compromete-se a cumprir integralmente a Resolução CMN nº 4.893/2021 (e suas sucessoras) e as diretrizes da LGPD.

- **Due Diligence de Fornecedores**: Realizar uma avaliação rigorosa de segurança e conformidade da LGPD em todos os fornecedores que tratarão dados pessoais em nome do Grupo Presença, antes da contratação.
- **Contratos Robustos**: Assegurar que os contratos com terceiros incluam cláusulas claras sobre proteção de dados, responsabilidades, medidas de segurança exigidas, direito de auditoria e procedimentos para tratamento de incidentes, conforme mencionado na *Politica de Privacidade dos Dados - Grupo Presença, Seção 15: Ações Internas do Grupo Presença para Proteção de Dados*, no item "Contratos com Terceiros".
- **Verificação Contínua**: Auditar e monitorar periodicamente os provedores de serviços para garantir a manutenção dos níveis de segurança e conformidade.
- **Transferência Internacional de Dados**: Em caso de transferência internacional de dados pessoais, garantir a conformidade com os artigos 33 e 34 da LGPD e as salvaguardas necessárias, como cláusulas contratuais padrão ou transferência para países com nível adequado de proteção, conforme *Politica de Privacidade dos Dados - Grupo Presença, Seção 10: Transferência Internacional de Dados Pessoais*.

7. Responsabilidade e Comunicação

A segurança cibernética e a proteção dos dados pessoais são responsabilidades compartilhadas por todos no **Grupo Presença**.

- **Matriz de Responsabilidades**: Manter uma matriz clara de responsabilidades e funções para a segurança cibernética e proteção de dados, definindo quem é responsável pelo quê e quais ações devem ser tomadas.
- **Comitê de Segurança e Privacidade**: Estabelecer um comitê multidisciplinar com representantes de TI, Jurídico, Compliance e o DPO para supervisionar a implementação e a manutenção das políticas de segurança e privacidade.
- **Canais de Comunicação Abertos**: Fomentar uma cultura que encoraje a comunicação proativa de vulnerabilidades, incidentes ou preocupações de segurança.
- **Compromisso da Alta Administração**: A alta administração do **Grupo Presença** compromete-se com a melhoria contínua dos processos e controles relacionados nesta Política, fiscalizando e auditando Operadoras de Dados conforme detalhado na *Política de Privacidade dos Dados - Grupo Presença, Seção 16: Responsabilidade pelo Tratamento dos Dados*.

8. Legislação Aplicável

Esta Política de Segurança Cibernética será regida, interpretada e executada de acordo com as Leis da República Federativa do Brasil, em especial a **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**. Adicionalmente, observará rigorosamente todas as regulamentações, normativos, circulares e resoluções emitidas pelos órgãos reguladores e fiscalizadores do setor financeiro e de mercado de capitais, incluindo o **Banco Central do Brasil (BACEN)**, a **Comissão de Valores Mobiliários (CVM)** e as normas do **Conselho Monetário Nacional (CMN)**, como a **Resolução CMN nº 4.893/2021** (e suas sucessoras), conforme *Política de Privacidade dos Dados - Grupo Presença, Seção 17: Legislação Aplicável*.

- **Monitoramento Regulatório**: O **Grupo Presença** manterá um monitoramento constante das mudanças na LGPD, nas regulamentações específicas do BACEN, CVM e CMN, e nas orientações da ANPD.
- **Assessoria Jurídica**: Contará com assessoria jurídica especializada para garantir que as políticas e práticas estejam sempre alinhadas à legislação vigente.

9. Disposições Finais

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

Ao interagir, cadastrar-se, fornecer seus dados ou, de qualquer forma, relacionar-se com o **Grupo Presença**, o Titular declara estar plenamente ciente, entender e concordar com o conteúdo integral desta Política, bem como com os termos estabelecidos, as finalidades e as bases legais para o tratamento de seus dados pessoais pelo **Grupo Presença**.

10. Vigência e Revisão

Esta Política de Segurança Cibernética entra em vigor a partir de **05/10/2025**.

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

11. Aprovação

Esta Política de Segurança Cibernética foi formalmente aprovada pela Alta Administração e liderança técnica do Grupo Presença, atestando o compromisso da organização com a segurança da informação e a proteção dos dados pessoais.