1. Objetivo

1.1 Estabelecer diretrizes de segurança da informação, segurança cibernética, segurança física de ambientes e de pessoas, segurança de canais, produtos e serviços, privacidade e proteção de dados pessoais, continuidade de negócios, e tratamento de dados e informações aplicáveis a todos os usuários dos ativos de informação, inclusive os do Conglomerado CAIXA.

1.2 Orientar as práticas de gerenciamento de dados e nortear as ações de segurança contra ameaças e ataques, em consonância com a Estratégia Corporativa do Conglomerado CAIXA, e propiciar conformidade com a legislação vigente.

2. Motivação

2.1 Atendimento à Instrução Normativa nº 1, de 27/05/2020, do Gabinete de Segurança Institucional da Presidência da República, e Resolução CVM nº 35, de 26/05/2021, quanto ao estabelecimento da Política da Segurança da Informação, à Resolução CGPAR/ME nº 41, de 04/08/2022, e CGPAR/ME nº 48, de 06/09/2023, quanto à manutenção das práticas de governança e ao estabelecimento de diretrizes e parâmetros para a gestão de riscos.

2.2 Atendimento à Resolução CMN n.º 4.557, de 23/02/2017, quanto à exigência de previsão de políticas e estratégias, claramente documentadas para a gestão de continuidade de negócios, à Instrução Normativa nº 3, de 28/05/2021, do Gabinete de Segurança Institucional da Presidência da República, quanto à gestão de Segurança da Informação e ao atendimento das diretrizes institucionais para gestão de Continuidade de Negócios.

2.3 Atendimento à Lei nº 13.709, de 14/08/2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.4 Atendimento à Resolução CMN nº 4.893, de 26/02/2021, quanto ao estabelecimento da política de segurança cibernética.

2.5 Aderência aos objetivos estratégicos do Plano Estratégico Institucional.

3. Vigência

3.1 A vigência desta política é de 01 (um) ano, podendo ser alterada quando o(s) gestor(es) identificar(em) necessidade de aprimoramento, considerando o ambiente regulatório, contexto macroeconômico ou necessidade estratégica, além de eventual determinação

advinda de órgãos reguladores e de fiscalização, ou por solicitações do colegiado o qual aprovou a matéria.

4. Diretrizes

4.1 Segurança da Informação

4.1.1 Os dados e as informações são ativos essenciais para a CAIXA e são protegidos para assegurar o seu uso de forma adequada, garantindo sua disponibilidade, integridade, confidencialidade e autenticidade na realização dos objetivos da CAIXA.

4.1.2 As informações da CAIXA, dos clientes e do público em geral são tratadas de acordo com boas práticas de mercado, sendo adotadas medidas técnicas e administrativas de Segurança da Informação.

4.1.3 As informações são classificadas conforme sua criticidade, sensibilidade e requisitos legais, de acordo com as normas internas vigentes.

4.1.4 A CAIXA comunica a ocorrência de incidentes relevantes de segurança de acordo com sua criticidade e requisitos legais.

4.1.5 Todos os ativos e serviços de informação, recursos computacionais da CAIXA, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet, são de uso exclusivo para o desempenho das atividades laborais e estão sujeitos à monitoração.

4.1.6 O uso dos recursos computacionais, o acesso remoto à internet, à computação em nuvem, às redes sociais e comunicadores instantâneos são realizados exclusivamente por meio de soluções tecnológicas disponibilizadas pela CAIXA, previamente homologadas e parametrizadas para a devida proteção das informações.

4.1.6.1 O tratamento de informações corporativas e de clientes por meio de comunicadores instantâneos é efetuado por meio de comunicadores aprovados pelas áreas de tecnologia e segurança.

4.1.7 A prática de “Mesa Limpa, Tela Limpa e Impressora Limpa” é adotada por todos os usuários, seja nas dependências da CAIXA ou em ambiente de trabalho remoto.

4.1.8 Os contratos, convênios e acordos operacionais que impliquem manuseio de informações da CAIXA possuem cláusula de confidencialidade e a obrigatoriedade de assinatura de Termo de Responsabilidade de Segurança e Informação da CAIXA, pelos colaboradores da contratada ou conveniada.

4.1.9 Os contratos, convênios e acordos operacionais que impliquem manuseio de informações sob a responsabilidade da CAIXA possuem cláusula que prevê a

obrigatoriedade da adoção de procedimentos de Segurança da Informação e treinamentos periódicos adequados e compatíveis com a natureza de suas atividades.

4.1.10 Os ambientes físicos e lógicos são criados e geridos de forma compatível com a confidencialidade das informações neles tratadas, inclusive com segregação de ambiente e controles de acesso adequados.

4.1.11 O acesso à informação é condizente com o critério de menor privilégio, no qual o usuário tem acesso somente às informações imprescindíveis para o desempenho de suas atribuições na Instituição.

4.1.12 O planejamento estratégico institucional da CAIXA contempla a gestão de segurança da informação.

4.1.13 A CAIXA mantém estruturas de governança e gestão de riscos de segurança da informação adequadas à natureza e complexidade de suas operações e produtos, e à dimensão de sua exposição a esse tipo de risco.

4.1.14 A CAIXA dissemina e mantém cultura de segurança e de uso correto da informação para seus usuários, inclusive, por meio de Testes de Phishing e ações de sensibilização contra demais ameaças.

4.1.15 As diretrizes dispostas nesta Política não são negociáveis e sua inobservância implica nas sanções previstas na legislação vigente e nas normas internas da CAIXA.

4.1.16 Unidade responsável: Diretoria Executiva Riscos.

4.2 Governança de Dados

4.2.1 Na CAIXA, a governança de dados estabelece as estratégias, as políticas e os objetivos atinentes ao gerenciamento de dados, relativamente à qualidade de dados ao uso efetivo e à disponibilidade, monitorando sua execução por meio de indicadores e incentivando o avanço e aperfeiçoamento das práticas de gestão de dados.

4.2.2 Na CAIXA, todos os dados possuem unidades administrativas responsáveis, designadas como Gestoras da Informação, que asseguram a organização, catalogação, qualidade, segurança, disponibilidade e integridade dos dados, contemplando os dados mestres e dados de referência gerenciados por regramento específico.

4.2.3 A CAIXA administra os riscos decorrentes das atividades de gestão de ativos de informação, de acordo com a estrutura organizacional e mandatos vigentes.

4.2.4 Os dados da CAIXA, bem como aqueles sob sua responsabilidade, são ativos estratégicos e devem ser utilizados, com intuito de elevar a eficiência e a inteligência analítica, impulsionando as estratégias negociais e a geração de resultados sustentáveis,

sendo compartilhados como um recurso para toda a empresa, de acordo com a necessidade de atuação das áreas.

4.2.5 A inserção, manuseio, o processamento, modificação ou alteração de dados corporativos ou de clientes são apenas os previstos em normas e processos.

4.2.6 Unidade responsável: Diretoria Executiva Clientes, Canais, Inteligência de Dados e Inovação.

4.3 Privacidade

4.3.1 Os dados pessoais são propriedade dos seus titulares, aos quais é garantido o exercício dos direitos previstos na LGPD.

4.3.2 A CAIXA zela pelo direito à privacidade, pela qualidade dos dados pessoais dos titulares e pela transparência em relação ao tratamento de dados pessoais que realiza.

4.3.3 Todo tratamento de dados pessoais realizado pela CAIXA se enquadra em hipótese legal aplicável, atendendo a propósito legítimo, específico, explícito, de acordo com a finalidade do tratamento justificada, documentada e devidamente informada ao titular.

4.3.4 O tratamento de dados pessoais realizado pela CAIXA limita-se ao mínimo necessário, abrangendo estritamente os dados pertinentes, proporcionais e não excessivos para o alcance de sua(s) finalidade(s).

4.3.5 A CAIXA não realiza o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

4.3.6 A privacidade, a segurança e seus respectivos controles são considerados e influenciam desde a etapa de concepção, documentação, prospecção e desenho de processos, produtos e serviços de negócio, bem como soluções, arquiteturas, ferramentas e serviços tecnológicos.

4.3.7 A CAIXA dissemina e mantém cultura de privacidade e proteção de dados pessoais.

4.3.8 Unidade responsável: Diretoria Executiva Riscos.

4.4 Segurança Cibernética

4.4.1 O gerenciamento de segurança cibernética é parte integrante e fundamental nas atividades da CAIXA.

4.4.2 O programa de segurança cibernética da CAIXA é pautado em inovação, automação, inteligência e boas práticas de mercado, a fim de manter a segurança da informação.

4.4.3 A CAIXA adota iniciativas de compartilhamento de informações sobre os incidentes de segurança cibernética relevantes com outras instituições financeiras e/ou parceiros externos.

4.4.4 São adotados critérios de decisão baseados nas estratégias e no gerenciamento de riscos para terceirização de serviços de segurança cibernética.

4.4.5 A gestão de riscos cibernéticos compreende a identificação de ameaças, vulnerabilidades, estimativa de impactos e a definição de ações voltadas ao monitoramento, análise e reportes internos.

4.4.6 São elaborados cenários de incidentes de segurança cibernética a serem considerados nos testes dos planos de continuidade operacional de TIC.

4.4.7 A CAIXA adota padrões e critérios de segurança tecnológica para gestão do acesso lógico aos recursos computacionais e protege as informações corporativas de acessos, alterações e compartilhamentos indevidos.

4.4.8 A CAIXA gerencia e protege a identidade lógica dos usuários internos e externos.

4.4.9 A CAIXA implementa controles e parâmetros seguros no uso da rede tecnológica, soluções e dispositivos corporativos.

4.4.10 O desenvolvimento seguro de sistemas é guiado por boas práticas de segurança cibernética no ciclo de desenvolvimento de sistemas e serviços.

4.4.11 Os sistemas da CAIXA possuem trilha de auditoria para rastreabilidade de ações e irregularidades executadas nos sistemas de informação ou por exigência legal, respeitando o sigilo e a confidencialidade das informações.

4.4.12 A gestão de incidentes de segurança cibernética leva em consideração a identificação, análise, contenção, erradicação e recuperação de ativos de TI.

4.4.13 A CAIXA mantém prontidão e processos definidos para resposta adequada a incidentes de segurança cibernética, atuando continuamente no monitoramento e análise dos controles de proteção da infraestrutura tecnológica.

4.4.14 A detecção de vulnerabilidades no ambiente cibernético da CAIXA abrange a utilização de testes e varreduras periódicos.

4.4.15 Unidade responsável: Diretoria Executiva Serviços TI.

4.5 Segurança Física e de Pessoas

4.5.1 A CAIXA zela pela integridade e segurança de empregados, clientes, colaboradores, visitantes nos seus ambientes físicos de atendimento, relacionamento e negócios e de seu patrimônio.

4.5.1.1 A definição dos equipamentos e procedimentos de segurança atribuídos aos ambientes físicos na CAIXA, considera as vulnerabilidades e a criticidade das atividades realizadas em cada área de uma unidade, e trata com o devido sigilo os dados dos usuários desses ambientes.

4.5.1.2 O acesso e circulação em ambientes físicos da CAIXA são registrados e monitorados com objetivo de resguardar a segurança de clientes, colaboradores, visitantes, ambientes físicos, informações e os materiais neles contidos.

4.5.1.3 A CAIXA privilegia o aperfeiçoamento técnico do corpo funcional, de forma contínua e permanente, promovendo o conhecimento para mitigação de ocorrências de segurança.

4.5.2 A CAIXA mantém representação junto aos órgãos de Segurança Pública, comunidades de inteligência e outras Instituições Financeiras para troca de experiências e adoção de parcerias para a prevenção e tratamento de ocorrências de segurança física e de pessoas.

4.5.3 Unidade responsável: Diretoria Executiva Logística, Contratação e Segurança.

4.6 Segurança de Produtos, Serviços e Canais

4.6.1 Alinhada à gestão de riscos operacionais, as Unidades Gestoras implementam estratégias de prevenção, mitigação, detecção e reação às ocorrências de segurança.

4.6.2 A CAIXA estimula a prospecção contínua de novas soluções de segurança, a análise recorrente de cenários, ameaças e vulnerabilidades e realiza a avaliação prévia de novas estratégias de produtos, serviços, processos, canais e atividades.

4.6.3 A CAIXA mantém representação junto aos órgãos de Segurança Pública, comunidades de inteligência e outras Instituições Financeiras para troca de experiências e adoção de parcerias para a prevenção e tratamento de ocorrências de segurança de produtos, serviços e canais.

4.6.4 A CAIXA sensibiliza seus clientes quanto à segurança na utilização de seus produtos e serviços.

4.6.5 Quando identificada ocorrência importante de segurança, iminente ou em curso, a CAIXA adota medidas imediatas de mitigação e contenção do risco, em conjunto com as Unidades Gestoras e dando conhecimento aos membros da Alta administração pertinentes.

4.6.6 Unidade responsável: Diretoria Executiva Logística, Contratação e Segurança.

4.7 Continuidade de Negócios

4.7.1 Os processos e serviços críticos de TIC são protegidos visando a continuidade de negócios da CAIXA.

4.7.2 São estabelecidos e testados regularmente planos de continuidade para os processos críticos identificados por meio de análise de impacto de negócios.

4.7.3 Os processos sustentados por terceiros, quando relevantes, possuem planos de continuidade de negócios.

4.7.4 Unidade responsável: Diretoria Executiva Riscos.

5. Responsabilidades

5.1 É responsabilidade de todos os usuários, Unidades da CAIXA e do Conglomerado aplicar as diretrizes desta política.

5.1.1 As empresas do conglomerado que, em função da sua natureza jurídica e/ou de aspectos legais, encontram-se impossibilitadas de aplicar as diretrizes aqui estabelecidas, deverão obter anuência expressa dos responsáveis por estas diretrizes, explicitando os pontos de conflito legais.

5.2 É responsabilidade de todos os usuários manter sigilo de informações relacionadas a ocorrências de segurança que venham a ter conhecimento em razão do exercício de suas atividades, tanto em âmbito interno quanto externo à CAIXA, excetuando-se a divulgação aos gestores das áreas envolvidas e/ou impactadas pela ocorrência.

5.3 O usuário é responsável pela proteção de suas senhas e dos demais mecanismos utilizados no controle de acesso aos sistemas da CAIXA, pois são pessoais, intransferíveis e o qualificam como responsável pelas ações realizadas, sendo vedado o compartilhamento destes com terceiros.

5.4 Caberá ao CDO (*Chief Data Officer*) viabilizar a definição e o monitoramento e fomentar a execução das diretrizes contidas nesta Política para a governança de dados na CAIXA.

5.5 É responsabilidade das unidades coordenadoras do Programa de Continuidade de Negócio da CAIXA e do Programa de Continuidade de Tecnologia da Informação e Comunicação aplicar a Análise de Impacto de Negócios, monitorar o desempenho dos indicadores do programa e realizar ações de aculturamento junto às unidades gestoras de processos e sistemas críticos.

5.6 É responsabilidade das unidades gestoras de processos críticos e de serviços críticos de TI definir estratégia de continuidade e construir planos de continuidade, testando-os de acordo com a periodicidade fixada em norma específica.

5.7 É responsabilidade da unidade gestora atuar, em conjunto com as áreas de segurança, na prevenção, identificação, mitigação ou controle dos riscos inerentes aos seus produtos, serviços, à proteção das informações, dos processos e/ou dos canais sob sua gestão.

5.8 Todas as Unidades da CAIXA são responsáveis pela adequação de seus processos, produtos, serviços e soluções tecnológicas aos requisitos da LGPD.

5.9 É responsabilidade do usuário registrar nos canais oficiais de comunicação da CAIXA todas as solicitações de informações e todas as informações fornecidas que envolvam dados corporativos e pessoais e/ou de clientes, contemplando registros de solicitações verbais, físicas ou digitais, documentos, comunicações, agendas de compromissos internos/externos e e-mails relacionados.

5.10 É responsabilidade do usuário denunciar e comunicar às Unidades Gestoras ou às áreas de segurança pertinentes, quando tiver conhecimento de tratamento de dados e informações em desconformidade com esta Política e demais situações que possam resultar em sua violação.

5.11 É responsabilidade do usuário ler e assinar o Termo de Responsabilidade de Segurança da Informação e o Termo de Ciência do Programa de Governança de Dados, conforme forma e periodicidade estabelecidas em normas específicas.

5.12 Cabe ao gestor da informação atuar na classificação, na definição de seus dados, metadados, perfis e regras de acesso, de suas finalidades de uso e salvaguardas de privacidade, na categorização dos dados pessoais, bem como nas regras para a manutenção da qualidade dos dados e informações sob sua responsabilidade.

5.12.1 No caso de unidades da matriz, o gestor chefe possui responsabilidade integral sobre as informações de sua unidade (enquanto estiver designado, sem prejuízo das disposições normativas internas e legais), estando encarregado de facilitar o compartilhamento de seus dados, promover a Governança de Dados e efetuar a gestão dos dados sob a ótica de controle e riscos em todas as etapas do ciclo de vida do dado no papel de 1ª Linha de Defesa.

5.13 É responsabilidade dos gestores dessa Política promover a sua disseminação, implementação e gestão.