POL-11	**POLÍTICA** DE SEGURANÇA CIBERNÉTICA	Revisão: 00
Responsabilidade: Diretoria de Operações e TI		Publicação: 05/01/2023
Aprovação: Conselho de Administração		Validade: 05/01/2026

I - OBJETIVO

Estabelecer diretrizes para garantir a proteção e manutenção das informações de propriedade Caixa Capitalização (nome fantasia da XS4 Capitalização S.A), levando em consideração a confidencialidade, integridade e disponibilidade, além de prevenir e mitigar vulnerabilidades ao ambiente de segurança cibernética.

II - ABRANGÊNCIA

Aplica-se a todos os Membros, Colaboradores e Parceiros de Negócio que utilizam recursos computacionais de propriedade da Caixa Capitalização.

III - REFERÊNCIAS

ABNT ISO/IEC 27001: 2013
ABNT ISO/IEC 27002: 2015
Circular SUSEP nº 638/2021
Circular SUSEP nº 635/2021
CIS Version 8
National Institute of Standards and Technology
Política de Gestão de Continuidade do Negócio
Política de Segurança da Informação para Parceiros de Negócio

IV - GLOSSÁRIO

Alta Administração: Refere-se ao Conselho de Administração e à Diretoria da Caixa Capitalização.

Área de Defesa Cibernética: Área interna do prestador de serviços responsável pela proteção do perímetro, análise de vulnerabilidade e resposta a incidentes.

Área de Segurança da Informação: Área interna do prestador de serviços responsável pela governança da segurança da informação, gestão de identidade, segurança em nuvem, proteção de dados e arquitetura de segurança.

Ativo Crítico: São os ativos que suportam a operação dos Processos Críticos.

Ativo de Informação: Todo elemento que agregue valor ao negócio, podendo ser uma informação digital ou física, hardware, pessoa ou ambiente físico, cuja quebra de confidencialidade, integridade ou disponibilidade poderá causar impacto aos negócios da Caixa Capitalização.

Colaboradores: São todos os funcionários, estagiários e aprendizes da Caixa Capitalização.

Confidencialidade: Princípio que limita o acesso à informação apenas às pessoas e entidades autorizadas, de forma legítima, pelo proprietário da informação.

Data Loss Prevention (DLP): Tecnologia utilizada para realizar inspeção e análise contextual de dados e executar respostas com base em políticas estabelecidas para prevenção a perda de dados.

Disponibilidade: Princípio que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Gestor da Informação: Aquele que de alguma forma, total ou parcialmente, zela pela administração, armazenamento, operação e preservação de um sistema ou dado estruturado.

Incidentes de Segurança da Informação: Qualquer evento adverso confirmado ou sob suspeita relacionado a segurança da informação, ocasionando o comprometimento de um ou mais princípios básicos da segurança, Confidencialidade, Integridade e Disponibilidade.

Integridade: Princípio que corresponde a preservação da precisão, consistência e confiabilidade das informações e sistemas da Caixa Capitalização ao longo dos processos ou de seu ciclo de vida.

Malware: Malware ou software malicioso, é um termo genérico para qualquer tipo de software de computador com intenção maliciosa. É qualquer software intencionalmente feito para causar danos a um computador, seja ele servidor ou cliente, ou até mesmo a uma rede de computadores.

Membros: São os membros do Conselho de Administração, do Conselho Fiscal, os membros externos indicados para ocupar os Comitês especiais de assessoramento ao Conselho de Administração e os Diretores Executivos.

MFA (Múltiplo Fator de Autenticação): É um método de autenticação que exige a utilização de dois ou mais fatores para liberação de acesso em algum sistema ou recurso computacional.

Parceiros de Negócios: São todos os parceiros comerciais públicos e privados, prestadores de serviços e qualquer outra pessoa, física ou jurídica, com quem a Caixa Capitalização mantenha relações comerciais.

Processo Crítico: Processo considerados essenciais para a continuidade do negócio da empresa, conforme definido no BIA (Análise de Impactos de Negócio).

RBI: Do inglês Remote Browser Isolation, o isolamento de navegador remoto (RBI) é uma tecnologia de segurança da Web que neutraliza ameaças online hospedando sessões de navegação na Web dos usuários em um servidor remoto em vez do dispositivo de terminal do usuário. O RBI separa o conteúdo da Web do dispositivo do usuário para reduzir sua superfície de ataque.

Single Sign-On: onde o usuário digita sua senha quando realiza o primeiro acesso e depois vai utilizando outras aplicações sem necessidade de digitar a senha novamente.

Threat Intelligence: Serviço de inteligência avançada de ameaças, que tem como objetivo, identificar e analisar indicadores de comprometimentos associados aos ambientes da Caixa Capitalização.

Usuário: Membros, Colaboradores e prestadores de serviço que tenham acesso a qualquer Informação em decorrência de suas atividades e prestação de serviços para a Caixa Capitalização seja em ambiente próprio ou terceirizado, localizado dentro ou fora das instalações da Caixa Capitalização.

V - DIRETRIZES

1 DIRETRIZES DE SEGURANÇA CIBERNÉTICA

1.1 A Segurança cibernética zela especificamente da informação tratada no ambiente digital. É a capacidade de identificar, prevenir, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.

1.2 Os ativos de informação são considerados bens de extrema importância para a Caixa Capitalização e devem ser tratados por todos com responsabilidade e comprometimento, permitindo que a sua confidencialidade, integridade e disponibilidade sejam preservadas, assegurando que o uso e compartilhamento destes ativos sejam controlados, sendo realizado o gerenciamento e tratamento dos incidentes provenientes de ataques cibernéticos.

1.3 A Alta Administração tem como compromisso garantir a Segurança Cibernética e a melhoria contínua dos processos, procedimentos e controles a ela relacionados.

1.4 Cabe à Diretoria de Operações e Tecnologia promover a cultura de segurança na Caixa Capitalização, desenvolvendo a conscientização e capacitação de Membros e Colaboradores para um uso responsável dos ativos de informação da Companhia.

1.4 Cada Membro, Colaborador ou Parceiro de Negócio que acesse ou manipule as informações armazenadas pela Caixa Capitalização é responsável pela segurança destes ativos de informação, assim como todos os procedimentos realizados através de suas identificações de acesso.

2 CLASSIFICAÇÃO DOS DADOS, SERVIÇOS E INCIDENTES RELEVANTES

2.1 DADOS RELEVANTES

2.1.1 São os dados pessoais e dados pessoais sensíveis, conforme definido em legislação em vigor, dados relativos a clientes ou a processos críticos de negócio, bem como dados classificados como confidenciais ou altamente confidenciais, conforme Norma de Classificação e Proteção da Informação.

2.2 SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS RELEVANTES

2.2.1 São os serviços de armazenamento ou processamento de dados, inclusive de computação em nuvem, que envolvam acesso ou manipulação de Dados Relevantes, ou que suportem Processos Críticos de negócio.

2.3 INCIDENTES RELEVANTES

2.3.1 São eventos que decorrem ou não de atividades maliciosas, comprometendo a confidencialidade, integridade ou disponibilidade de dados relevantes, ou afetem sistemas de processamento ou armazenamento de dados que suportem atividades essenciais para a continuidade do negócio.

3 GESTÃO DE ACESSOS

3.1 O fluxo de gestão de acesso utiliza o controle, monitoramento e restrição seguindo os conceitos de menor privilégio (ou seja, conceder a um usuário o acesso apenas ao que é absolutamente necessário

para desempenhar suas responsabilidades e nada mais), revisão periódica e cancelamento imediato ao encerramento do vínculo com Membros e Colaboradores ou contrato com Parceiro de Negócio.

3.2 Os acessos às informações são rastreáveis, permitindo a identificação individual do Usuário quando acessadas ou manipuladas as informações.

3.3 Para evitar que um único responsável possa executar e controlar os processos críticos durante todo o seu ciclo de vida, é necessário realizar a segregação de funções.

3.4 Os Usuários possuem uma identificação única, pessoal e intransferível, tornando-o responsável por todas as ações realizadas nos sistemas da Caixa Capitalização.

3.5 Os Usuários criam uma senha, considerada como uma informação altamente confidencial, pessoal e intransferível, devendo ser utilizada como assinatura eletrônica, sendo estritamente proibido o seu compartilhamento.

3.6 Os acessos devem conter mecanismos de rastreabilidade, a fim de garantir que as ações de auditoria sejam capazes de identificar individualmente o Usuário e este responsabilizado por suas ações.

4 AUTENTICAÇÃO

4.1 O acesso às informações e aos dispositivos da Caixa Capitalização deve ser restrito apenas aos Usuários autorizados pelo Gestor da Informação, levando em consideração o princípio do menor privilégio, a segregação das funções críticas que geram conflitos e a classificação das informações.

4.2 Para garantir um gerenciamento de acesso adequado aos sistemas, é necessário contemplar os seguintes controles:

a) A utilização de credenciais de acesso individuais, sendo monitoradas e suscetível a bloqueios e restrições (automáticos e manuais);

b) A aplicabilidade de autenticação de múltiplo fator, sempre que possível;

c) A aplicabilidade de autenticação via Single Sign-On, sempre que possível;

d) A remoção de autorizações aos Usuários deligados ou afastados da Caixa Capitalização;

e) A remoção de autorizações aos Usuários que mudaram de função; e

f) A revisão periódica das autorizações atribuídas.

5 PROTEÇÃO DA INFORMAÇÃO

5.1 Toda informação gerada ou manipulada pelos Membros, Colaboradores ou Parceiros de Negócio são constituídas como ativos de propriedade da Caixa Capitalização, sendo consideradas essenciais para a condução de negócio. Esta deve ser utilizada unicamente à finalidade a qual foi destinada pelo Gestor da informação, devendo ser protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade.

5.2 A Caixa Capitalização conta com ferramentas de prevenção de perda de dados (DLP), sendo estas utilizadas na descoberta de dados em repouso, monitoramento de dados em trânsito e na gestão dos acessos, garantindo a mitigação de acessos indevidos.

5.3 Para proteger os Usuários de malware ou códigos maliciosos contidos em sites, são utilizadas tecnologias de isolamento remoto de navegadores, conhecida como RBI.

5.4 O serviço de *Threat Intelligence* visa identificar potenciais ameaças, sendo essas comunicadas a equipe de Defesa Cibernética. Para esses casos, é realizada a priorização da correção das vulnerabilidades de acordo com seu grau de criticidade, sendo corrigidas primeiramente em ambiente de homologação e, ao corrigir essas possíveis ameaças, são transportadas para o ambiente de produção.

6 PREVENÇÃO A VAZAMENTO DE INFORMAÇÃO

6.1 A Caixa Capitalização adota controles para prevenção de perda de dados, assegurando que as informações confidenciais tenham cópias de segurança e sejam armazenadas em ambientes seguros para evitar perdas, roubos, má utilização ou vazamento de informações na rede por Usuários não autorizados.

7 GESTÃO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

7.1 É realizado o monitoramento de segurança dos ativos de Hardware e Software pela Caixa Capitalização, onde são identificados e classificados os possíveis incidentes de acordo com seu grau de impacto.

7.2 Incidentes classificados como críticos devem ser analisados pela Área de Segurança da Informação, seu impacto mensurado e devidamente comunicado à alta direção, conforme descrito na Norma de Gestão de Incidente de Segurança da Informação.

7.3 Anualmente, a Companhia deverá elaborar relatório sobre prevenção e tratamento de incidentes, conforme critérios estabelecidos em normativo próprio sobre gestão de Incidentes de Segurança da Informação.

8 GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO

8.1 A Área de Segurança da Informação deverá estabelecer direcionadores para a realização da gestão de vulnerabilidade em normativo próprio, que aborde minimamente os domínios:

a) Gestão de Vulnerabilidade;
b) Correções de Segurança; e
c) Testes Periódicos de Segurança, incluindo testes de intrusão , phishing e de ransomware, dentre outros.

8.2 Essa abordagem visa identificar as vulnerabilidades no ambiente de tecnologia da informação da Caixa Capitalização para mitigar os riscos a serem priorizados e a redução do fator de exposição das ameaças cibernéticas. O mapeamento e classificação dos fatores de riscos, bem como seus controles internos e estabelecimento de matriz de riscos identificados, serão controlados em conjunto com a área de gestão de riscos internos.

9 DESENVOLVIMENTO SEGURO DE SOFTWARE

9.1 A Caixa Capitalização mantém um conjunto de princípios para o desenvolvimento seguro de sistemas de informação, garantindo que a prática de segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

9.2 O desenvolvimento seguro de software interno e terceirizado deverá respeitar os critérios a serem definidos em normativo próprio.

10 CORREIO ELETRÔNICO, AMBIENTE DE INTERNET E ANTI-MALWARE

10.1 A Caixa Capitalização disponibiliza aos Usuários a tecnologia necessária com o objetivo de facilitar a comunicação interna, com clientes, fornecedores e demais públicos de relacionamento. É de responsabilidade do Usuário a utilização da tecnologia de forma adequada, para fins corporativos, de modo compatível com as legislações, normas de órgãos reguladores e princípios aplicáveis aos negócios.

10.2 O acesso à internet é um serviço destinado apenas à execução de tarefas alinhadas aos negócios da Caixa Capitalização. As mensagens transmitidas através destes recursos são de propriedade da Caixa Capitalização independentemente de sua forma.

10.3 A Caixa Capitalização se reserva no direito de monitorar todos os acessos, mensagens de e-mail corporativo, uso de seus recursos, facilidades e autoridade relacionadas à Internet dos Usuários da Caixa Capitalização e qualquer ação identificada como inadequada, será informada ao Usuário e ao respectivo gestor.

10.4 Não é permitido o uso de e-mails pessoais através dos dispositivos e da infraestrutura da Caixa Capitalização.

10.5 O uso de rede wireless e rede cabeada para acesso à internet e a utilização de e-mail corporativo deverão ter suas regras definidas em normativo próprio.

10.6 Todos os ativos que estejam conectados à rede corporativa ou façam uso de informações da Caixa Capitalização devem, sempre que compatível, ser protegidos com uma solução anti-malware determinada pela Área de Segurança da Informação.

11 CRIPTOGRAFIA

11.1 Os ativos de hardware (Desktops e Notebooks) internos devem passar pelo processo de criptografia de disco, prevenindo o acesso de pessoas não autorizadas aos dados armazenados nos dispositivos da Caixa Capitalização.

11.2 Os dados confidenciais e altamente confidenciais que estejam em repouso e em trânsito devem utilizar mecanismos de criptografia, que será objeto de normativo próprio, visando estabelecer os níveis de confidencialidade conforme as regras estabelecidas na Norma de Classificação e Proteção da Informação e os padrões de segurança dos Órgãos Reguladores.

12 CÓPIAS DE SEGURANÇA (BACKUP)

12.1 Com o objetivo de assegurar a disponibilidade das informações, os dados gerados e armazenados nos ativos de informação da Caixa Capitalização são mantidos através de cópias de segurança, nomeadas como backup corporativo, visando evitar a perda de dados, erro de arquivos, falhas de mídias, entre outras ocorrências ou paradas não programadas, permitindo que estes possam ser recuperados e disponibilizados conforme estratégia de continuidade.

12.2 O processo de execução de backups é realizado, periodicamente, nos ativos de informação da Caixa Capitalização, as regras relativas à execução das cópias de segurança das informações e de recuperação dos dados armazenados estão descritas na Norma de Gestão de Backup.

13 DIRETRIZES DE SEGURANÇA AOS USUÁRIOS

13.1 AUTENTICAÇÃO E SENHA

13.1.1 Os Usuários que recebem um login e senha exclusivos para realizar a autenticação nos sistemas internos da Caixa Capitalização são responsáveis pelos atos executados com suas credenciais.

13.1.2 É dever dos Usuários:

a) O não compartilhamento de senha;
b) A memorização da senha;
c) A alteração periódica da senha ou sempre que houver suspeitas quanto ao comprometimento dela;
d) A criação de senhas complexas, contendo letras maiúsculas, minúsculas, números e caracteres especiais;
e) O bloqueio do equipamento durante ausências da estação de trabalho;
f) Impedir o uso do login por outras pessoas;
g) A restrição quanto ao uso de senhas com privilégios administrativos;
h) A autenticação do Usuário utilizando o Single Sign-On, sempre que possível;
i) Sempre que possível, utilizar o MFA (Múltiplo fator de autenticação).

13.2 TESTE DE SEGURANÇA

13.2.1 São realizados testes durante o processo de desenvolvimento e mudança de estrutura de software com o objetivo de mitigar vulnerabilidades durante a codificação nos sistemas de informação desenvolvidos internamente pela Caixa Capitalização.

13.2.2 Para proporcionar maior segurança aos sistemas da Caixa Capitalização, os softwares internos e de fornecedores, são constantemente avaliados, através de testes de intrusão executados pelo time interno e por empresas parceiras. Os processos de teste devem ser executados com periodicidade de 3, 6 ou 12 meses, conforme descrito em normativo próprio.

13.3 ENGENHARIA SOCIAL

13.3.1 A Engenharia Social é comumente aplicada por criminosos que utilizam da manipulação e persuasão a pessoas desavisadas ou sem muita experiência no mundo virtual para obter informações confidenciais, infectar os equipamentos ou obter acesso não autorizado a informações corporativas.

13.3.2 Para evitar ataques de Engenharia Social, a Caixa Capitalização realiza o controle por ferramentas de e-mail, filtrando os conteúdos recebidos internamente e mitigando eventos de segurança cibernética que possam comprometer a organização.

13.4 PHISHING

13.4.1 Phishing é uma técnica muito utilizada por cibercriminosos para enganar os Usuários, enviando e-mails para coletar informações pessoais, financeiras ou corporativas e até mesmo infectar o dispositivo da vítima.

13.4.2 As maneiras de persuasão utilizadas através do Phishing podem variar de acordo com as seguintes abordagens:

a) Apresentar vantagens financeiras aos Usuários, buscando chamar a atenção da vítima;
b) Se passar por comunicações oficiais de instituições conhecidas, como: Bancos, Lojas de Comercio Eletrônico, entre outros;
c) Através da indução ao preenchimento de formulários com informações pessoais, corporativas (Usuário e senha de rede) e/ou financeiras;
d) Instalação de softwares maliciosos com o intuito de coletar informações sensíveis dos Usuários.

13.4.3 Buscando prevenir ataques Phishing, a Caixa Capitalização conta com ferramentas de filtro de conteúdo para identificar e reportar e-mails suspeitos à Área de Segurança da Informação.

13.5 SPAM

13.5.1 Os Spams são os principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

13.5.2 Buscando prevenir a disseminação de e-mails Spam, a Caixa Capitalização conta com uma ferramenta de contenção que realiza o filtro destes e-mails.

13.6 DISPOSITIVOS DE ARMAZENAMENTO USB

13.6.1 Referente ao uso de Dispositivos USB, é proibido:

a) A utilização de dispositivos USB pessoais ou não homologados pela Caixa Capitalização;
b) Conectar dispositivo USB da Caixa Capitalização em um dispositivo pessoal;
c) A utilização de dispositivos USB desconhecidos;
d) A utilização de dispositivos USB infectados.

13.6.2 Em casos de exceção, os dispositivos de armazenamento USB são liberados para Usuários que necessitem para atividades pertinentes ao desempenho de suas atividades profissionais, sendo

permitido apenas dispositivos homologados pela Caixa Capitalização. É realizada uma varredura de antivírus nesses dispositivos.

13.7 COMUNICAÇÃO DE ATIVIDADES MALICIOSAS

13.7.1 Caso qualquer Usuário possua a confirmação ou suspeita de que suas senhas aos sistemas da Companhia ou Dispositivos USB tenham sido comprometidas, bem como tenha sido vítima de Engenharia Social, Phishing, Spams ou qualquer outro tipo de atividade maliciosa, devem comunicar à Área de Segurança da Informação por meio de algum dos seguintes canais:

a) equipedefesacibernetica@icatuseguros.com.br;
b) Equipe Service Desk;
c) csirt@caixacapitalização.com.br.

14 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

14.1 Conforme a Circular 638/2021, da Superintendência de Seguros Privados - SUSEP para a contratação de serviços de processamento e armazenamento de dados, a Caixa Capitalização deve assegurar que possui direcionadores e controles para a aderência aos requisitos de segurança cibernética previstos na regulamentação em vigor.

14.3 Todos os Parceiros de Negócio que em razão de suas atividades manuseiem informações da Caixa Capitalização deverão cumprir as disposições da Política de Segurança para Parceiros de Negócio.

14.4 Todos os serviços relevantes de processamento ou armazenamento de dados deverão ser informados à SUSEP em até 30 (trinta) dias após a formalização dos contratos, contendo todas as informações exigidas pelas regulamentações vigentes.

14.5 A Caixa Capitalização conta com diretrizes que determinam as responsabilidades e obrigações atribuídas ao provedor de serviço de hospedagem em nuvem. Assim como a adoção de processos para relatar incidentes e falhas de segurança com seus fornecedores, tais quais devem ser documentadas, controladas e comunicadas a todas as partes afetadas.

14.6 O provedor de serviço de soluções em nuvem deve relatar como os Incidentes de Segurança são tratados e atribuir responsabilidades para atender os requisitos de segurança da Companhia. A Caixa Capitalização deverá dispor em normativos específicos sobre os padrões mínimos de conformidade e governança para utilização de serviços em nuvem.

14.7 Os fornecedores que durante a avaliação de segurança da informação forem classificados com risco alto devem ser devidamente reportados à área de gestão de riscos corporativos para validação da Alta Administração.

15 PENALIDADES

15.1 A Área de Segurança da Informação se reserva o direito de preventivamente suspender os acessos dos Usuários que estiverem realizando quaisquer atividades em desacordo com essa política.

15.2 Quando identificado uma violação das regras estabelecidas nesta política, este deverá ser tratado como incidente de segurança e analisado pela área responsável conforme as políticas e diretrizes estabelecidas pela Caixa Capitalização.

15.3 Em caso de descumprimento das regras, o Usuário terá seu acesso aos sistemas de informação, rede e banco de dados removidos e a área de Recursos Humanos será notificada de tal infração. O acesso só será reestabelecido após aprovação do Diretor responsável pelo Usuário.

15.4 Cada Usuário é responsável por seus atos no uso dos recursos computacionais oferecidos. Assim, o Usuário poderá responder por qualquer consequência decorrente do uso indevido e/ou descumprimento da presente política, seja nas esferas administrativa ou judicial.

VI - HISTÓRICO DE REVISÃO

REVISÃO	DATA	DESCRIÇÃO DA REVISÃO
00	02/08/2022	Redação inicial.

VII – HISTÓRICO DE APROVAÇÃO

DATA	ATA DA REUNIÃO
28/12/2022	Ata da Reunião do Conselho de Administração de 28/12/2022.