POLÍTICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

1 PREMISSAS 1

2 OBJETIVO 1

3 ABRANGÊNCIA 2

4 CONCEITOS 2

5 DIRETRIZES GERAIS 2

6 RESPONSABILIDADES: 3

6.1 ÓRGÃO DE ADMINISTRAÇÃO 3

São responsabilidades do Conselho de Administração: 3

6.2 DIRETOR RESPONSÁVEL PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA 3

6.3 GERÊNCIA / GESTOR 4

6.4 ÁREA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA 4

6.5 SÃO RESPONSABILIDADES DOS COLABORADORES 4

7 PRINCÍPIOS E PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA 5

7.1 SERVIÇOS DE COMPUTAÇÃO EM NUVEM 5

7.2 Estrutura Tecnológica 5

7.3 CONTROLE DE SENHAS 6

7.4 RELACIONAMENTO COM TERCEIROS 6

7.5 CLASSIFICAÇÃO DA INFORMAÇÃO 7

7.6 CONTROLE E RESTRIÇÃO DE ACESSO 7

7.7 COMUNICAÇÕES DE RISCOS 7

7.8 ACULTURAMENTO 7

7.9 CONTINUIDADE DOS NEGÓCIOS 7

7.10 PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA 8

7.10.1 EQUIPE DE RESPOSTA AO INCIDENTE 8

7.10.2 IDENTIFICAÇÃO DO INCIDENTE 8

7.10.3 TRIAGEM DO INCIDENTE 8

7.10.4 ANÁLISE DO INCIDENTE 9

7.10.5 CATEGORIZAÇÃO E PRIORIZAÇÃO DO INCIDENTE 9

7.10.6 MITIGAÇÃO DO INCIDENTE 10

7.10.7 CONTENÇÃO DO INCIDENTE 10

7.10.8 IDENTIFICAÇÃO DE CAUSA E SOLUÇÃO 10

7.10.9 RESPOSTA AO INCIDENTE 11

7.10.10 AÇÕES PÓS-INCIDENTE 11

7.11 RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA AOS INCIDENTES 12

7.12 MONITORAMENTO 12

8 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM 13

8.1 EXIGÊNCIAS PARA CONTRATAÇÃO DE SERVIÇOS 13

8.2 AVALIAÇÃO PRÉVIA DOS SERVIÇOS 15

8.3 CONTRATOS COM PRESTADORES DE SERVIÇOS 15

8.4 COMUNICAÇÃO AO BANCO CENTRAL 18

9 DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL 18

10 PROTEÇÃO E PREVENÇÃO DE RISCOS CIBERNÉTICO 19

11 TRATAMENTO DE INCIDENTES 19

12 DECLARAÇÃO DE RESPONSABILIDADE 20

Os contratos firmados com a Coopluiza devem possuir cláusula que assegure a confidencialidade das informações protegidas por sigilo e pela legislação e regulamentação vigentes. 20

13 DIVULGAÇÃO 20

14 VIOLAÇÃO DA POLÍTICA E SANÇÕES 21

15 TREINAMENTO 21

16 REVISÃO 21

17 CONSIDERAÇÕES FINAIS 21

1 PREMISSAS

O presente documento constitui uma declaração formal da **COOPERATIVA DE CRÉDITO MÚTUO DOS EMPREGADOS DO MAGAZINE LUIZA, EMPRESAS CONTROLADAS E COLIGADAS – COOPLUIZA** acerca de seu compromisso em orientar e seguir um conjunto de regras definidas de maneira objetiva, mantendo uma estrutura de Segurança da Informação que assegura a integridade, a disponibilidade e a confidencialidade dos dados, inclusive nos casos de contratação de serviços específicos, visando a adequação ao exigido na Resolução CMN nº 4.893/2021 e a Resolução BACEN nº 85/2021.

2 OBJETIVO

O objetivo desta Política é assegurar a proteção dos ativos de informação da COOPLUIZA contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de nossos negócios, com o intuito de aplicar os princípios e diretrizes de proteção das informações consideradas sensíveis da instituição e de seus clientes e colaboradores.

A COOPLUIZA se compromete, por meio dessa Política, a oferecer os recursos necessários à melhoria contínua dos procedimentos relacionados à segurança cibernética, mantendo, com o menor risco possível, um ambiente computacional seguro.

Para atingir o objetivo, são determinados procedimentos internos destinados a minimizar a ocorrência de riscos cibernéticos e para identificar violações de segurança cibernética, estabelecendo ações sistemáticas de controles, registros, detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos.

A COOPLUIZA garante a confidencialidade, integridade e disponibilidade da informação em todo o seu ciclo de vida: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte.

3 ABRANGÊNCIA

As diretrizes, normas, princípios e valores presentes na presente Política se aplicam a toda COOPLUIZA, devendo, assim, serem conhecidas e cumpridas por todos os conselheiros, gerentes, gestores, colaboradores, fornecedores e terceiros.

4 CONCEITOS

a) segurança cibernética: é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a internet e telefones celulares;

b) ativos de informações: são todas as informações geradas ou desenvolvidas para o negócio, e podem estar presentes em diversas formas, tais como: arquivos digitais, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, bancos de dados e conversas;

c) incidentes: qualquer ocorrência que não é parte padrão da operação de um serviço e que pode causar uma indisponibilidade, redução na qualidade dele, perda de integridade ou confidencialidade das informações;

d) risco cibernético: ameaça à confidencialidade, integridade e disponibilidade das informações.

5 DIRETRIZES GERAIS

A Política de Segurança Cibernética é orientada como parte essencial e integrada aos processos de negócios, com o objetivo primordial da consecução dos objetivos e metas empresariais, atendendo as exigências legais e os controles estabelecidos são entendidos como oportunidade de melhoria nos padrões éticos e na transparência das informações.

Como forma de reduzir as vulnerabilidades dos ativos de informação, a COOPLUIZA adota procedimentos e os controles baseados em:

- Autenticação;
- Criptografia;
- Prevenção e detecção de intrusão;
- Prevenção de vazamento de informações;
- Testes e varreduras para detecção de vulnerabilidades;

- Proteção contra *softwares* maliciosos;
- Mecanismos de rastreabilidade;
- Controles de acesso e segmentação de rede de computadores;
- Manutenção de cópias de segurança dos dados e das informações.

Os procedimentos e os controles devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição.

6 RESPONSABILIDADES:

6.1 ÓRGÃO DE ADMINISTRAÇÃO

São responsabilidades do Conselho de Administração:

a) aprovar esta política de segurança cibernética, o plano de ação e de respostas de incidentes;

b) prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética;

c) manter comprometimento e apoio à aderência a política de segurança cibernética de acordo com os objetivos e estratégias de negócio estabelecidas para organização;

d) fornecer à área de segurança da informação e cibernética claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário;

fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança cibernética.

6.2 DIRETOR RESPONSÁVEL PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA

São responsabilidades do diretor responsável pela política de segurança cibernética:

a) propor melhorias nas diretrizes da política de segurança cibernética e no plano de ação;

b) acompanhar se as diretrizes da política estão sendo executadas;

c) executar o plano de ação e de respostas de incidentes.

6.3 GERÊNCIA / GESTOR

São responsabilidades dos gestores

a) garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança de cibernética;

b) avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;

c) designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;

d) autorizar acessos de seus colaboradores apenas quando forem realmente necessários.

6.4 ÁREA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

São responsabilidades da Área de Segurança da Informação e Cibernética:

a) desenvolver e estabelecer programas de conscientização e divulgação da política de segurança cibernética;

b) conduzir o processo de gestão de riscos de segurança cibernética;

c) conduzir a gestão de incidentes de segurança cibernética, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

d) conduzir a definição controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas;

e) propor projetos e iniciativas para melhoria do nível de segurança das informações da cooperativa.

6.5 SÃO RESPONSABILIDADES DOS COLABORADORES

São responsabilidades dos Colaboradores:

a) notificar a área segurança da informação e cibernética os incidentes de segurança que venha a tomar conhecimento e as violações desta política de segurança cibernética;

b) utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de segurança cibernética.

7 PRINCÍPIOS E PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

A implementação desta política considera o porte, perfil de risco e modelo de negócios da cooperativa, considerando suas operações, produtos, serviços e processos atuais e ainda para atender a esta política baseia -se nos seguintes princípios:

a) confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

b) integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);

c) disponibilidade: garantir que as informações estejam disponíveis às pessoas autorizadas.

7.1 SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Em atendimento a Resolução nº. 4893/21 os serviços de computação em nuvem da abrange:

a) empregar de recursos computacionais dos prestadores de serviços em casos de implantação, execução de aplicativos adquiridos ou desenvolvidos pela cooperativa;

b) processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos que permitam a cooperativa implantar e executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos;

c) usar de recursos computacionais do próprio prestador de serviços para execução por meio de internet dos aplicativos implantados ou desenvolvidos.

Na gestão dos serviços contratados devem ser avaliados a confiabilidade, integridade, disponibilidade, segurança e sigilo das informações, os recursos utilizados, bem como o cumprimento da legislação vigente.

7.2 Estrutura Tecnológica

A COOPLUIZA oferece aos Colaboradores completa estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho e pelo controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Equipamentos disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da cooperativa. As mensagens enviadas ou recebidas através do correio eletrônico corporativo, seus respectivos anexos e a navegação na internet, através de equipamentos da COOPLUIZA, poderão ser monitoradas.

A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da COOPLUIZA depende de autorização do Gerente da área e do responsável pela Política de Segurança Cibernética.

A empresa dispõe de Política de Segurança da Informação e Política de BYOD (*Bring Your Own Device)*, que deverão ser observadas para realização dos procedimentos.

7.3 CONTROLE DE SENHAS

As senhas para acesso aos equipamentos e sistemas são pessoais e intransferíveis, não devendo ser divulgados para terceiro, sob pena de responsabilização.

As senhas não devem ser anotadas ou armazenadas; não devem ser baseadas em informações pessoais e devem ser complexas, com alterações periódicas, inclusive caso haja suspeita de acesso indevido.

7.4 RELACIONAMENTO COM TERCEIROS

Os prestadores de serviço, fornecedores e empresas conveniadas devem adotar procedimentos e controles compatíveis com os riscos envolvidos na prestação de serviços relevantes prestados junto aos clientes, preservando, inclusive, a continuidade das operações e negócios da COOPLUIZA, contando com Termos de Confidencialidade das Informações e condições específicas, considerando a realidade de cada contratação. A empresa dispõe de Política de Relacionamento com Terceiros, que deverá ser observada para realização dos procedimentos.

7.5 CLASSIFICAÇÃO DA INFORMAÇÃO

As informações são classificadas de acordo com a confidencialidade e as proteções necessárias e, devem ser tratadas de forma sigilosa, de acordo com a regulamentação e a legislação vigentes, observada a finalidade do tratamento. A empresa dispõe de Política de Classificação de Informações, que deverá ser observada para realização dos procedimentos relacionados.

7.6 CONTROLE E RESTRIÇÃO DE ACESSO

O acesso às informações só deve ser feito se devidamente autorizado, e o acesso deverá ser realizado por meio de credencial única, pessoal, intransferível e identificável, conforme a Política de Segurança da Informação da COOPLUIZA.

7.7 COMUNICAÇÕES DE RISCOS

Quaisquer riscos às informações dos clientes da COOPLUIZA devem ser comunicados diretamente à diretoria ou através dos canais de atendimento oferecidos pela COOPLUIZA aos seus clientes.

A empresa dispõe de Política de Gestão de Riscos, que deverá ser observada para realização dos procedimentos relacionados.

7.8 ACULTURAMENTO

A COOPLUIZA atuará na disseminação da cultura de segurança cibernética, incluindo a conscientização dos seus clientes e usuários de produtos e serviços.

7.9 CONTINUIDADE DOS NEGÓCIOS

A COOPLUIZA mantém procedimentos específicos relacionados à Continuidade do Negócios, contemplados na Política de Continuidade de Negócios e no Plano de Continuidade de Negócios, que engloba, ainda, o Plano de Recuperação de Desastres, visando assegurar a continuação de seus negócios, em caso de paralisação decorrente de sinistro, de um ou mais processos considerados críticos.

7.10 PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

7.10.1 EQUIPE DE RESPOSTA AO INCIDENTE

A Equipe de Resposta ao incidente será composta de representantes da Coopluiza, preferencialmente com cargo de gestão (gerentes e gestores) e representantes da equipe de TI Magalu – Luiza Labs.

7.10.2 IDENTIFICAÇÃO DO INCIDENTE

Consiste em detectar ou identificar de fato a existência de um incidente de segurança Cibernética. A Equipe de Resposta ao Incidente baseia-se na identificação de incidentes internos ou externos, seja na detecção de alertas provenientes dos sistemas de monitoramento da rede da COOPLUIZA ou por notificações realizadas por qualquer pessoa relatando ser de seu conhecimento ou mesmo vítima de atividade suspeita ou em desacordo com a Política de Segurança Cibernética.

As notificações internas ou externas devem ser realizadas por meio de: a) Registro de Denúncia ou suspeita de incidente no link do site https://www.coopluiza.com.br/lgpd.

Toda notificação ou denúncia deve ser formalmente registrada pela Gerência de Riscos – Coopluiza. Este registro deve estar associado a alguma referência numérica (ID único) para que possa ser gerenciado pela Equipe de Resposta ao Incidente, conforme modelo de formulário.

7.10.3 TRIAGEM DO INCIDENTE

Etapa onde a Equipe de Resposta ao Incidente deve realizar a análise inicial do evento, notificação ou denúncia visando a sua confirmação como incidente e classificando a sua relevância sobre as atividades da Coopluiza. Nesta Etapa deve ser identificados os sintomas do evento, suas características e os potenciais danos causados.

Confirmado que um incidente foi detectado, ele deve ser analisado antes de qualquer ação seja tomada, principalmente para confirmar se é um incidente válido.

7.10.4 ANÁLISE DO INCIDENTE

A análise realizada pela Equipe de Resposta ao Incidente consiste na coleta, aquisição e análise de dados, informações e demais evidências sobre o incidente para investigar o ativo de rede ou sistema de informação que gerou o incidente detectado ou denunciado.

Essa investigação passa pela identificação de ativos compreendendo endereços IP, endereços MAC da interface de rede, nomes, switches. Essas informações devem ser levantadas pelas trilhas de auditoria dos diversos sistemas e serviços disponíveis pela COOPLUIZA.

7.10.5 CATEGORIZAÇÃO E PRIORIZAÇÃO DO INCIDENTE

Confirmado o incidente, a Equipe de Resposta ao Incidente deve categorizar e priorizar com base: (i) no impacto potencial que pode ter sobre a COOPLUIZA; (ii) no tempo e recursos necessários para recuperar ativos impactados. O impacto potencial deve ser identificado com base na tabela identificada na Política de Segurança da Informação da COOPLUIZA.

Todo incidente categorizado como sendo de severidade crítica deve ser notificado imediatamente ao Diretor de Riscos Cibernéticos, que pode realizar a escalação deste incidente e realizar a alocação dos profissionais necessários para resolução do incidente.

Caso o incidente detectado envolva ou tenha a suspeita de envolver o tratamento não autorizado de dados pessoais, a Equipe de Resposta ao Incidente deve notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais (DPO) para avaliar se o incidente informado se trata de uma violação de dados pessoais.

Confirmado que o incidente é uma violação de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais (DPO) deve ser adicionado na Equipe de Resposta ao Incidente para orientar e acompanhar as medidas a serem tomadas.

Se mais de um incidente estiver ocorrendo ao mesmo tempo, os incidentes devem ser priorizados, pois não haverá o tempo e recursos para atuar simultaneamente.

Nesta etapa, a Equipe de Resposta ao Incidente deve apresentar as ações que serão priorizadas com base na categoria e no impacto do cenário encontrado e realizar as comunicações necessárias.

7.10.6 MITIGAÇÃO DO INCIDENTE

Etapa que busca a solução do incidente por meio de um ciclo básico composto pelas seguintes fases: (i) análise dos dados, (ii) pesquisa de solução, (iii) ação proposta e realizada (contenção), (iv) comunicação, (v) solução efetiva ou de contorno e (vi) recuperação do ambiente.

7.10.7 CONTENÇÃO DO INCIDENTE

Devem ser realizados procedimentos iniciais para contenção do incidente visando evitar a sua propagação e posteriormente em restabelecer o ativo, mesmo que com uma solução temporária, até que a solução definitiva seja implementada.

A Equipe de Resposta ao Incidente deve assegurar que as comunicações com Partes Internas e Externas Interessadas ocorram no momento oportuno e estejam coordenadas de acordo com as diretrizes de gestão de crises da COOPLUIZA. As Partes Interessadas Internas devem ser informadas sobre as ações que precisam ser realizadas durante o estágio de recuperação.

7.10.8 IDENTIFICAÇÃO DE CAUSA E SOLUÇÃO

A Equipe de Resposta ao Incidente deve buscar a solução definitiva, ou seja, identificar a causa raiz de um incidente e eliminá-lo para assegurar que o ativo esteja seguro e confiável para que os procedimentos de recuperação sejam iniciados. A Equipe de Resposta ao Incidente pode solicitar o envolvimento e suporte das demais Áreas da COOPLUIZA afetadas para assegurar que os vetores do incidente sejam solucionados.

A Equipe de Resposta ao Incidente deve acompanhar os processos de recuperação dos ativos até o pleno funcionamento.

Os sistemas relevantes da COOPLUIZA devem retomar a funcionalidade básica de modo prioritário. As interdependências sistêmicas também devem ser conhecidas, já que alguns sistemas só podem ser recuperados após outros.

Durante a recuperação, os sistemas devem ser reconstruídos, reinstalados ou restaurados pela área de TI usando dados de backup e sistemas e patches atualizados, se necessário com apoio da Equipe de Resposta ao Incidente. Os sistemas recuperados devem ser testados e monitorados para assegurar que não ocorra novamente o incidente e que os ativos estejam funcionando de modo adequado.

7.10.9 RESPOSTA AO INCIDENTE

Equipe de Resposta ao Incidente deve documentar e arquivar as conclusões do tratamento do incidente, descrevendo:

a) o que aconteceu;
b) como o incidente foi detectado, ou seja, foi relatado por pessoal natural ou por um alerta de sistema automatizado;
c) as etapas tomadas pela Equipe de Resposta ao Incidente a partir da detecção do evento até o estágio de recuperação dos ativos;
d) o status do incidente à medida que ele se move ao longo do processo de solução;
e) qualquer dado que seja coletado durante o processo de solução que possa ser usado como evidência;
f) definir a categorização final do incidente;
g) comentários e sugestões da Equipe de Resposta ao Incidente.

Esta documentação deve servir como referência para pós-incidente.

A coleta e preservação de prova na etapa de solução do incidente, bem como dados e informações que possibilitaram a identificação do incidente são importantes e devem ser documentadas no registro final do incidente. A coleta de provas deve ser avaliada conforme a necessidade pela Equipe de Resposta ao Incidente, devendo acionar o Jurídico em caso de dúvidas quanto à sua necessidade.

Quando um incidente for categorizado como severidade crítica deve ser realizada a coleta e preservação das provas envolvidas.

7.10.10 AÇÕES PÓS-INCIDENTE

A etapa de pós incidente tem o seu início após a resolução e encerramento do incidente, onde serão analisadas pela Equipe de Resposta ao Incidentes causas que motivaram a sua ocorrência e quais são as medidas que podem ser tomadas com objetivo que o fato não ocorra novamente.

O objetivo desta etapa é melhorar os procedimentos realizados na etapa de resposta e aprimorar os ativos para protegê-los de futuros incidentes.

A Equipe de Resposta ao Incidente deve comunicar as partes interessadas do resultado da análise.

Os incidentes ocorridos devem ser analisados em conjunto com os procedimentos de continuidade de negócio e governança de dados pessoais da COOPLUIZA. Esta análise visa identificar aprimoramento dos indicadores de

probabilidade e consequência dos incidentes previstos e as ocorrências reais de incidentes.

Com base no relatório e nas informações obtidas durante a solução do incidente, a Equipe de Resposta ao Incidente deve criar um plano de ação que incluam os responsáveis, datas de vencimento e entregas para garantir que todas as partes interessadas saibam o que se espera delas. As ações devem ser categorizadas como curto ou longo prazo.

7.11 RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA AOS INCIDENTES

A equipe de resposta a incidentes em conjunto com o DPO e com apoio das áreas relacionadas elaborarão um relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data base de 31 de dezembro.

O relatório deverá conter no mínimo as seguintes informações:

- resumo dos resultados alcançados na implementação de rotinas, procedimentos e tecnologias utilizados na prevenção e na resposta a incidentes;
- a efetividade alcançada na implementação desta política;
- as ocorrências de incidentes relevantes ocorridos no período relacionado referente ao ambiente cibernético;
- resultados de testes de continuidade de negócios;

O relatório deverá ser apresentado ao Conselho de Administração ou, à diretoria da instituição até 31 de março do ano seguinte ao da data-base.

7.12 MONITORAMENTO

São criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da COOPLUIZA através das seguintes ações:

- Inventários atualizados de *hardware* e *software*, com verificação de frequência para identificar elementos estranhos à instituição.
- Sistemas operacionais e *softwares* de aplicação atualizados, instalando as atualizações disponibilizadas;

- Monitoramento rotinas de *backup*, executando testes regulares de restauração dos dados, conforme Política de *Backup* instituída pela COOPLUIZA;
- Realização, periodicamente testes de invasão externa e *phishing*;
- Realização análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura;
- Testes periódicos do plano de resposta a incidentes, simulando os cenários.

A efetividade da Política de Segurança Cibernética é verificada por meio de avaliações independentes periódicas de auditoria interna e externa, incluindo órgãos de controle e reguladores.

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

Os Prestadores de serviços e parceiros de serviços de processamento de dados e armazenamento em nuvem podem representar uma fonte significativa de riscos de cibersegurança.

A computação em nuvem considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações, envolve determinados riscos que são levados em conta pela COOPLUIZA, demandando assim cuidados proporcionais.

8.1 EXIGÊNCIAS PARA CONTRATAÇÃO DE SERVIÇOS

A COOPLUIZA, ao realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as seguintes exigências:

a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, considerando a criticidade do serviço e sensibilidade das informações, observando, inclusive, a classificação das informações;

b) Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:

- Cumprimento da legislação e da regulamentação em vigor;
- Permissão de acesso da COOPLUIZA aos dados e as informações a serem processadas ou armazenadas pelo Prestador de serviços;
- Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo Prestador de serviços;
- Aderência a certificações que a COOPLUIZA possa exigir para a prestação do serviço a ser contratado;
- Acesso da COOPLUIZA aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
- Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;
- Identificação e segregação dos dados dos clientes COOPLUIZA por meio de controles físicos ou lógicos;
- Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados da COOPERATIVA.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela cooperativa, deve observar os seguintes requisitos:

- A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- Assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;
- Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
- Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anterior a COOPLUIZA deverá solicitar autorização do Banco Central do Brasil para a contratação, em até 60 (sessenta) dias antes da alteração contratual.

A COOPLUIZA deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações, com documentação que evidencie as condições.

8.2 AVALIAÇÃO PRÉVIA DOS SERVIÇOS

A COOPLUIZA deve proceder a uma avaliação da relevância dos serviços prestados por empresas com possibilidades de serem contratadas considerando o seguinte:

- Criticidade dos serviços a serem prestados.
- Sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada.
- Verificação quanto a adoção, por parte do prestador de serviços quanto a adoção de controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet.

8.3 CONTRATOS COM PRESTADORES DE SERVIÇOS

Os contratos firmados entre a COOPLUIZA e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) A indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

b) A adoção de medidas de segurança para a transmissão e armazenamento dos dados;

c) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

d) A obrigatoriedade, em caso de extinção do contrato, de:

Transferência dos dados ao novo prestador de serviços ou a cooperativa.

Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

e) O acesso da COOPLUIZA a:

- Informações fornecidas pela empresa contratada visando verificar o cumprimento dos itens previstos nos itens a), b) e c) acima.
- Informações relativas às Certificações exigidas pela COOPLUIZA e aos relatórios de auditoria especializada contratada pelo prestador de serviços.
- Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f) A obrigação da empresa contratada notificar a COOPLUIZA sobre a subcontratação de serviços relevantes para a Cooperativa.

g) A permissão de acesso do Banco Central do Brasil às seguintes informações:

- Contratos e acordos firmados para a prestação de serviços;
- Documentação e informações referentes aos serviços prestados;
- Dados armazenados;
- Informações sobre processamento;
- Cópias de segurança dos dados e das informações;
- Códigos de acesso aos dados e as informações.

h) A adoção de medidas pela COOPLUIZA em decorrência de determinação do Banco Central do Brasil;

i) A obrigatoriedade de a empresa contratada manter a COOPLUIZA permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor;

j) O contrato deve também prever, para o caso de decretação de regime de resolução da COOPLUIZA pelo Banco Central:

- A obrigação da empresa contratada para a prestação de serviços conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada.
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:
  - A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime da resolução.
  - A notificação prévia deve ocorrer também na situação em que a interrupção for motivava por inadimplência da Cooperativa.

Complementarmente, recomenda-se que as avaliações e contratos, ainda, observem os seguintes critérios:

a) Estar atuando no mercado há, no mínimo, 3 (três) anos, tendo, preferencialmente, experiência no segmento de Cooperativas de Crédito;

b) Empresa deve seguir recomendações internacionais e boas práticas de segurança da informação;

c) O contrato estabelecido com a empresa deverá contemplar condições relacionadas ao nível de serviço (ANS – Acordo de Nível de Serviço ou SLA – *Service Level Agreement*), com detalhamento do nível técnico e operacional, contemplando a segurança dos dados armazenados, prazo do serviço, ferramentas utilizadas, metas mensuráveis do desempenho do trabalho prestado, tipo de formato do suporte técnico, requisitos para acessos, como autenticação multifatorial e demais informações relevantes;

8.4 COMUNICAÇÃO AO BANCO CENTRAL

A COOPLUIZA deverá informar previamente ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada com até 10 dias após a contratação dos serviços e deve conter as seguintes informações:

a) denominação da empresa a ser contratada;
b) os serviços relevantes a serem contratados
c) a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

As alterações contratuais que impliquem modificações nas informações contratuais devem ser comunicadas ao Banco Central no mínimo 10 dias após a alteração contratual.

9 DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- Política de Segurança Cibernética;
- Ata de Reunião do Conselho de Administração da COOPLUIZA implementada a Política de Segurança Cibernética;
- Documento relativo ao Plano de ação e de resposta a incidentes relativos à implementação da Política de Segurança Cibernética;
- Relatório anual sobre a implementação do Plano de ação e de resposta a incidente;
- Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra;

- Contratos de Prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem;
- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

10 PROTEÇÃO E PREVENÇÃO DE RISCOS CIBERNÉTICO

As ações de proteção e prevenção da cooperativa a fim de manter funcionamento e efetividade da segurança cibernética seguem os seguintes requisitos:

a) manter relatório de inventários de *hardware* e *software*;

b) verificar com frequência se há na cooperativa computadores não autorizados ou *software* não licenciado;

c) manter os sistemas operacionais e *software* atualizados;

d) realizar frequentemente testes de invasão externa e *pishing*;

e) fazer análises de vulnerabilidade na estrutura tecnológica da cooperativa frequentemente ou em situações que houver mudança significativas;

f) fazer teste do plano de resposta a incidentes com simulação de cenários.

11 TRATAMENTO DE INCIDENTES

Os incidentes são interrupções de sistema tecnológico não planejados que afetam os negócios das cooperativas e podem acontecer nas seguintes situações;

a) queda de energia;

b) falha de um elemento de conexão ou servidor fora do ar;

c) ausência de conexão com a internet;

d) terrorismo;

e) ataques de DDOS;

f) indisponibilidade de acesso a cooperativa.

As ocorrências de incidentes devem ser avaliadas com relação a gravidade da situação, os motivos que levaram aos acontecimentos desses incidentes e as consequências para os negócios da cooperativa.

A cooperativa deverá realizar as seguintes ações após a avaliação dos incidentes:

a) avaliar o impacto do incidente na cooperativa;

b) redirecionar as linhas de telefones para os celulares, instruir o provedor de telefonia a desviar linhas de dados, entre outros;

c) avaliar a relevância, em caso de sabotagem ou terrorismo a fim de decidir pelo registro de boletim de ocorrência ou outras providencias caso seja necessário;

d) comunicar tempestivamente ao Banco Central do Brasil (BCB) as ocorrências de incidentes relevantes e as interrupções de serviços relevantes que configurem uma situação de crise na cooperativa.

Após o incidente ter sido resolvido com a contingência da segurança cibernética e demais equipes chaves notificados, as áreas devem verificar se os dados estão faltando ou foram corrompidos ou outros problemas.

Caso seja identificado que a cooperativa perdeu informações ou dados, os diretores e equipe de contingência da cooperativa devem ser informados imediatamente e na retomada dos processos deverão ser definidos ações que incluem a análise de procedimentos para que a cooperativa possa operar normalmente, bem como reconstrução de eventuais sistemas e mudanças e medidas de prevenção.

12 DECLARAÇÃO DE RESPONSABILIDADE

Os colaboradores e prestadores de serviços diretamente contratados pela Coopluiza devem aderir formalmente a um termo comprometendo-se a agir de acordo com a Política de Segurança Cibernética.

Os contratos firmados com a Coopluiza devem possuir cláusula que assegure a confidencialidade das informações protegidas por sigilo e pela legislação e regulamentação vigentes.

13 DIVULGAÇÃO

Para uniformidade da informação, a Política de Segurança Cibernética deve ser divulgada após aprovação pelo Conselho de Administração, seja na sua constituição ou em quaisquer atualizações que se façam necessárias.

Adicionalmente, deve ser disponibilizada na empresa, permitindo fácil acesso ou consulta aos colaboradores. A política também deve ser divulgada para novos colaboradores, no processo de integração.

Esta Política entra em vigor na data de sua publicação, ficando revogadas quaisquer disposições em contrário.

14 VIOLAÇÃO DA POLÍTICA E SANÇÕES

O descumprimento das diretrizes desta política, mesmo que por mero desconhecimento, sujeitará o infrator à sanções administrativas, incluindo a aplicação de advertência verbal ou escrita, suspensão, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

15 TREINAMENTO

A Coopluiza deve estabelecer um programa de conscientização em Segurança Cibernética à garantia dos objetivos e diretrizes definidos nesta Política a fim de apresentar às necessidades e responsabilidades específicas de cada colaboradores.

16 REVISÃO

Esta política será revisada anualmente pelo setor de Planejamento e Compliance e sua aprovação caberá ao Conselho de Administração.

17 CONSIDERAÇÕES FINAIS

O Conselho de Administração compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta Política.

Os indícios ou irregularidades devem ser comunicadas a área de segurança da informação e cibernética.

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e prestadores de serviços com abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

Esta política é aprovada Conselho de Administração e comunicada a todos os colaboradores e partes interessadas que sejam relevantes para o cumprimento necessário.

Esta política foi aprovada na reunião do Conselho de Administração realizada em 14/11/2023 e registrada na ata de nº 152029.

18 CONTROLE DE ATUALIZAÇÕES

Data	Item atualizado	Descrição
14/11/2023	Item 7.10	Implementação do Plano de Ação e de Resposta à Incidentes de Segurança Cibernética
14/11/2023	Item 7.11	Correção da data de criação e apresentação ao conselho de administração do relatório anual de implementação do plano de ação e de segurança cibernética.

POLÍTICA DE SEGURANÇA CIBERNÉTICA - COOPLUIZA V.11.2023.pdf

Documento número #b70b6399-a0ba-4549-a388-0ca874bbc6a9

Hash do documento original (SHA256): b1dc0afe82c2135f61afbaddc8856a24edfa4d2f645760e161ad975324b7feba

Assinaturas

Valéria Luiza Abreu de Araújo
Assinou em 27 nov 2023 às 22:15:16

Alexandro Buck
Assinou em 27 nov 2023 às 17:52:33

Vinícius Henrique Peraro
Assinou em 29 nov 2023 às 11:03:58

Log

27 nov 2023, 16:00:33	Operador com email fabio.santos@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 criou este documento número b70b6399-a0ba-4549-a388-0ca874bbc6a9. Data limite para assinatura do documento: 27 de dezembro de 2023 (15:58). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
27 nov 2023, 16:00:34	Operador com email fabio.santos@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 adicionou à Lista de Assinatura: valeria@magazineluiza.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Valéria Luiza Abreu de Araújo.
27 nov 2023, 16:00:34	Operador com email fabio.santos@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 adicionou à Lista de Assinatura: raquel.palma@magazineluiza.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Raquel de Souza Palma Lancha.
27 nov 2023, 16:00:34	Operador com email fabio.santos@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 adicionou à Lista de Assinatura: marilisediniz@magazineluiza.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Marilise Bertelli Diniz.
27 nov 2023, 16:00:34	Operador com email fabio.santos@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 adicionou à Lista de Assinatura: alexandro@magazineluiza.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alexandro Buck.

27 nov 2023, 16:00:34	Operador com email fabio.santos@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 adicionou à Lista de Assinatura: vinicius.peraro@fintechmagalu.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Vinícius Henrique Peraro.
27 nov 2023, 17:52:33	Alexandro Buck assinou. Pontos de autenticação: Token via E-mail alexandro@magazineluiza.com.br. IP: 200.232.53.218. Localização compartilhada pelo dispositivo eletrônico: latitude -23.5153949 e longitude -46.622282. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.676.0 disponibilizado em https://app.clicksign.com.
27 nov 2023, 22:15:16	Valéria Luiza Abreu de Araújo assinou. Pontos de autenticação: Token via E-mail valeria@magazineluiza.com.br. IP: 163.116.233.48. Localização compartilhada pelo dispositivo eletrônico: latitude -23.6750786 e longitude -46.670534. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.676.0 disponibilizado em https://app.clicksign.com.
29 nov 2023, 11:03:58	Vinícius Henrique Peraro assinou. Pontos de autenticação: Token via E-mail vinicius.peraro@fintechmagalu.com.br. IP: 189.90.138.134. Localização compartilhada pelo dispositivo eletrônico: latitude -20.5392025 e longitude -47.3971753. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.680.0 disponibilizado em https://app.clicksign.com.
30 nov 2023, 14:25:45	Operador com email priscila.vieira@coopluiza.com.br na Conta 8dafccf5-ceef-40e2-83b2-d73afefd89c3 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número b70b6399-a0ba-4549-a388-0ca874bbc6a9.