POLÍTICA DA ESTRUTURA SIMPLIFICADA DE

GERENCIAMENTO CONTÍNUO DE RISCOS

Cibernético

Conteúdo

1. INTRODUÇÃO

A **Política Da Estrutura Simplificada De Gerenciamento Contínuo De Risco Cibernético** da **COOPERATIVA DE CRÉDITO MÚTUO DOS EMPREGADOS DO MAGAZINE LUIZA, EMPRESAS CONTROLADAS E COLIGADAS – COOPLUIZA** tem por finalidade definir diretrizes para efetivar e para manutenção das estratégias, rotinas e procedimentos de gerenciamento de riscos cibernético.

A cooperativa mantém ***Estrutura Simplificada De Gerenciamento Contínuo De Riscos*** em atendimento a Resolução nº 4.557/17 e Resolução 4.606/17 com objetivo de *identificar*, *mensurar*, *avaliar*, *monitorar*, *reportar*, *controlar* e *mitigar* O RISCO CIBERNETICO que a instituição esteja **exposta de maneira relevante**, *considerando:*

i. O modelo de negócios, com a natureza das operações, complexidade dos produtos e serviços, das atividades e dos processos da Cooperativa;

ii. A dimensão e à relevância da exposição aos riscos, segundo critérios definidos pela Cooperativa.

iii. Adequada ao Perfil de riscos da Cooperativa.

A **COOPLUIZA** é uma cooperativa singular, classificada como "capital x empréstimo", segmentada como "S5", trata se de cooperativa fechada e opera oferecendo empréstimos lastreados no capital de seus cooperados que são somente as pessoas físicas com vínculo trabalhista das empresas do Magazine Luiza, empresas Coligadas e Controladas.

A política atende as exigências legais e os controles estabelecidos são entendidos como oportunidade de melhoria nos padrões éticos e na transparência das informações.

A **COOPLUIZA** mantém estrutura de TI que assegura a integridade, a segurança e a disponibilidade dos dados relativos ao gerenciamento de riscos.

A **COOPLUIZA** mantém a política de continuidade de negócios que esteja exposta de maneira relevante.

Os modelos e os procedimentos internos asseguram as operações realizadas através de procedimentos e pessoal qualificado para a função.

Todas as análises e procedimentos de risco serão reportados ao Conselheiro com função de Diretor de Risco que reportará ao Conselho de Administração.

A Coopluiza deverá manter atualizado o Relatório Gerencial versando sobre o desempenho da estrutura simplificada de gerenciamento de risco cibernético.

A documentação relativa à estrutura de gerenciamento de riscos cibernético ficará à disposição do Banco Central do Brasil por cinco anos.

2. O OBJETIVO E DEFINIÇÕES.

O objetivo desta Política é orientar a administração da COOPERATIVA na gestão da segurança da informação e cibernética, demonstrando o compromisso com a proteção das informações corporativas e demais ativos de informação, destinados a garantir a confidencialidade, integridade e disponibilidade das informações.

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 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.

Para esclarecimentos dessa política são definidos:

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 operação da cooperativa, 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.

3 PRINCIPIOS E VALORES

A cooperativa possui como princípios seu compromisso com a transparência e o respeito nas relações para com seus cooperados, usuários dos serviços cooperativos.

As informações dos usuários de serviços cooperativos são guardadas de acordo com padrões de confidencialidade e segurança, sendo compartilhados à terceiros, nos termos da lei, desde que necessários para a execução de serviços/operações contratadas e sob o dever de proteção de dados e confidencialidade dos mesmos.

Assim, como princípios e valores que norteiam essa política de Risco Cibernético são:

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 somente para executar o tratamento necessário.

4. CRITÉRIOS E PROCEDIMENTOS

4.1 ÁREAS ENVOLVIDAS / RESPONSABILIDADES

O Conselho de Administração é responsável pela política de Gerenciamento de Riscos Operacionais, devendo ser revisada e atualizada de maneira que demonstre e identifique preventivamente a existência de vulnerabilidades que possam expor a **COOPLUIZA** a riscos, considerados incompatíveis com os níveis de riscos aceitáveis, para que as ações sejam tomadas para reduzir essa exposição.

O Conselho de Administração, também continuamente mantém a correção de eventuais deficiências da estrutura simplificada de gerenciamento de riscos que possam ser identificadas, assegura a observância por todos na **COOPLUIZA.**

Compete **ao Conselho de Administração** no mínimo a cada dois anos aprovar e revisar as políticas e estratégias de gerenciamento de riscos operacional.

Cabe ao Conselho de administração prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética; promovendo a disseminação da cultura de gerenciamento de riscos por todos os participantes da **COOPLUIZA.**

Todo componente da estrutura organizacional da cooperativa, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações e deve cumprir as determinações desta política, normas e padrões de segurança cibernética.

A COOPLUIZA entende que é importante que cada colaborador deve focar na conformidade com as normas, leis, padrões e/ou procedimentos internos ou externos. Tudo isso com o propósito de mitigar as diversas vulnerabilidades às quais a cooperativa está sujeita.

Os Conselheiros de Administração em função executiva acompanham se as diretrizes da política estão sendo executadas e também se estão sendo desenvolvidos e implementados os planos de ação e de respostas de incidentes aprovados.

4.1.1 GERÊNCIA e COORDENADORES

A gerência, os coordenadores e os supervisores têm como responsabilidade:

a) assegurar que todos da equipe tenham acesso, conhecimento e implementação pratica desta política e demais normas e padrões de segurança de cibernética;

b) assegurar que o acesso a dados e informações pela equipe seja somente o necessário ao desempenho de suas funções, atribuições e para cumprimento das operações e atividades da cooperativa;

c) avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe, garantindo a confidencialidade, integridade e disponibilidade das informações.

d) 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;

e) Identificar com a equipe técnica as violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos;

Ainda que seja com o suporte de área técnica a Gerência será responsável em:

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.

4.1.2 COLABORADORES E PRESTADORES DE SERVIÇOS

Todos os colaboradores e prestadores que tenham qualquer acesso cibernético e as informação da Cooperativa será responsável:

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

b) Utilizar os dados pessoais de forma licita e somente para o que foi aprovado a sua utilização e não armazenar além do determinado no procedimentos operacionais da cooperativa.

c) 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;

4.2. Declaração de Responsabilidade

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

Seguindo as boas praticas, gradualmente deverá implementar aos contratos firmados com prestadores que tenham acesso cibernético e as informações da Cooperativa cláusula que assegure a confidencialidade das informações protegidas por sigilo e pela legislação e regulamentação vigentes.

4.3 Treinamento

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

A cooperativa em seus treinamentos a colaboradores e/ou integrações a novos colaboradores deverá conscientizar que todas as ações, sistemas, serviços, dados, informações disponíveis não devem ser interpretadas como sendo de uso pessoal, portanto, todos devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pelo departamento de TI, gestores ou por prestador de serviços externo.

5 . SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Os serviços de computação em nuvem abrangem:

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.

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

A computação em nuvem é uma forma de contratação de serviços de terceiros, e esses prestadores de serviços de processamento e armazenamento de dados representam um risco de cibersegurança para a cooperativa, sendo necessário cuidados em casos de identificação de ameaças.

Na contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior devem ser considerados os seguintes requisitos à empresa contratada:

a) ter Política de Segurança Cibernética e plano de continuidade de negócios – PCN;

b) manter registro e autorização em caso de mudanças ou alterações de serviços ou sistemas; e

c) ter relatórios de controles e gestão de incidentes.

A cooperativa continuamente verifica a capacidade potencial do prestador de serviços de processamento e armazenamento de dados e de computação em nuvem a fim de assegurar o cumprimento da legislação em vigor, permissão de acessos da cooperativa aos dados e as informações que serão processadas ou armazenadas.

O prestador de serviços de processamento e armazenamento de dados e de computação em nuvem deve manter a confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas e armazenadas.

A COOPLUIZA deverá ter acesso aos relatórios de auditoria contratada pelo prestador de serviço e fornecimento de informações e de recursos de gestão adequados aos monitoramentos dos serviços as serem prestados.

Os prestadores de serviços relevantes serão avaliados considerando a criticidade do tipo de serviços a ser prestado, bem como a sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas.

Ainda, devem ser verificadas a adoção de controles que reduzam eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados pela internet.

5.2 CONTRATOS COM PRESTADORES DE SERVIÇOS

Os contratos firmados com as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever a indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados que poderão ser armazenados, processados e gerenciados, bem como adoção de medidas de segurança para transmissão de armazenamento de dados.

Enquanto o contrato estiver vigente, deve prever a manutenção da segregação dos dados e dos controles de acessos para proteção das informações dos usuários dos serviços da cooperativa.

A empresa contratada deverá notificar a cooperativa sobre a subcontratação de serviços relevantes para a cooperativa.

A cooperativa deverá ter acesso às informações fornecidas pelas empresas contratadas visando verificar o cumprimento da indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados que poderão ser armazenados, processados e gerenciados, bem como adoção de medidas de segurança para transmissão de armazenamento de dados.

A empresa prestadora de serviço deverá disponibilizar a cooperativa o acesso as informações relativas ao relatório de auditoria especializada contratada pelo prestador de serviço e recursos de gestão adequadas ao monitoramento dos serviços contratados.

Os contratos devem prever ainda permissão de acesso ao Banco Central do Brasil – BCB nas seguintes informações;

a) contratos e aos acordos firmados para a prestação de serviços;

b) documentação e às informações referentes aos serviços prestados;

c) dados armazenados e às informações sobre seus processamentos;

d) cópias de segurança dos dados e das informações;

e) códigos de acesso aos dados e às informações;

f) adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e

g) obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

O contrato mencionado na alínea "a" deve prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

a) a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados na alínea "g" do caput, que estejam em poder da empresa contratada; e

b) a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

b.1) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

b.2 a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

6. AÇÕES DE 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.

g) A cooperativa realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, dentre as medidas, incluem-se:

- Verificação dos logs dos colaboradores;
- Alteração periódica de senha de acesso dos Colaboradores;
- Segregação de acessos;

h) A cooperativa deverá solicitar para os fornecedores testes e eficácia dos processos utilizados para evitar e revelar as principais vulnerabilidades dos sistemas que estão sob a responsabilidades deles, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real;

7. TRATAMENTO DE INCIDENTES

Os incidentes são interrupções de sistema tecnológico não planejado 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) indisponibilidade de acesso a cooperativa.

e) Indícios ou ocorrências com perda de dados, roubo ou vazados de dados,

f) terrorismo e ataques cibernéticos;

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 os contatos como 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 conselheiros com funções executivas e equipe de contingência da cooperativa devem ser informados imediatamente e na retomada dos processos deverão ser definidos ações que incluem a análise procedimentos para que a cooperativa possa operar normalmente, bem como reconstrução de eventuais sistemas e mudanças e medidas de prevenção.

8. RELATÓRIO DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES

A cooperativa deverá emitir anualmente o relatório de implementação de plano de ação e respostas a incidentes.

Os referidos relatórios devem ser aprovados pelos Conselheiros em função Executiva responsável pela segurança cibernética.

O relatório deverá ser emitido com data base de 31 de dezembro e conter, no mínimo, as seguintes informações:

a) resumo dos resultados alcançados na implementação de rotinas, procedimentos e tecnologias utilizados na prevenção e na resposta a incidentes;

b) as ocorrências de incidentes relevantes ocorrido no período relacionado referente ao ambiente cibernético;

8.1 DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA

Devem ficar à disposição do Banco Central do Brasil – BCB:

a) a presente Política;

b) a ata do Conselho de Administração com a aprovação da política;

c) documento relativo ao plano de ação e de resposta a incidentes;

d) relatório anual e a documentação sobre os procedimentos;

e) documentação que trata no caso de serviços prestados no exterior;

f) os contratos de prestação de serviços relevantes de processamento,

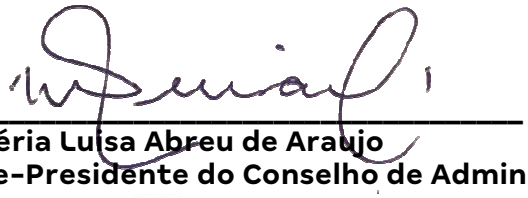
9. CONSIDERAÇÕES FINAIS

Essa Política será revisada em periodicidade de dois anos ou quando mudanças significativas exigirem.

Essa **Política Da Estrutura Simplificada De Gerenciamento Contínuo De Risco** está aprovada pelo Conselho de Administração na reunião de 25/08/2021.

Franca, 25 de agosto de 2021.

Vinícius Henrique Peraro
Presidente do Conselho de Administração



Valéria Luisa Abreu de Araujo
Vice-Presidente do Conselho de Administração

Marilise Bertelli Diniz
Vogal do Conselho de Administração