MAGICREDI Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro

Política de Segurança Cibernética e da Informação

Política atualizada e aprovada pela Diretoria da Cooperativa, conforme Resolução 4.893/21 do Banco Central do Brasil, em reunião ordinária realizada em 23 de agosto de 2023.

Av. Erasmo Braga nº 227 – Grupo 809 - Centro - Rio de Janeiro - RJ CEP: 20 020-000
Tel. / Fax: 2531-8539 E-mail - magicredi.rj@magicredi.com.br
Posto Tribunal – Av. Erasmo Braga, nº 115 - Lâmina 01- 4º andar - Centro – Rio de Janeiro- RJ
CEP. 20020-903 Tel. (21) 2531-8998 / (21) 2220-5014 – Ouvidoria 0800-282-8539

1. INTRODUÇÃO

A Política de Segurança Cibernética e da Informação da Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro – MAGICREDI-RJ é uma declaração formal da cooperativa acerca do seu compromisso com a proteção de Informações Confidenciais e Segurança Cibernética (*cybersecurity*), conforme definição adiante, devendo ser cumprida por todos os integrantes do seu quadro de atividades.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Confidenciais. Aprovada pela Diretoria Executiva da Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro - MAGICREDI-RJ, a Implementação da Política Institucional de Segurança Cibernética, conforme Resolução CMN nº. 4.893 de 26 de fevereiro de 2021 têm como objetivo atender as determinações do Banco Central do Brasil, que cumprindo decisão do Conselho Monetário Nacional, dispôs sobre a Política de Segurança Cibernética e sobre os Requisitos para a Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem a serem observados pelas Instituições Financeiras, cujos princípios, conceitos, valores e práticas serão adotados pelos administradores e demais membros estatutários, funcionários e colaboradores em geral da *COOPERATIVA DE CRÉDITO DOS MAGISTRADOS DO ESTADO DO RIO DE JANEIRO LTDA – MAGICREDI-RJ*, com base em princípios e diretrizes contidos neste documento, buscando assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Cooperativa.

2. PÚBLICO

Todos os usuários que compõem as estruturas organizacionais da entidade da Cooperativa de Crédito dos Magistrados - MAGICREDI-RJ (dirigentes, empregados e estagiários) e demais pessoas com acesso autorizado às informações da Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro - MAGICREDI-RJ, incluindo cooperados, parceiros, empresas prestadoras de serviço e ao público.

3. OBJETIVO

Esta Política visa proteger as Informações Confidenciais e a propriedade intelectual da MAGICREDI-RJ e de seus cooperados, bem como aprimorar a segurança cibernética da cooperativa, nos termos da Resolução nº 4.893, de 26 de fevereiro de 2021. Dessa forma, a Política Institucional de Segurança Cibernética da MAGICREDI-RJ visa:

I. Definir diretrizes para a segurança do espaço cibernético relacionadas à capacidade das entidades da Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro-MAGICREDI-RJ de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;

II. Proteger as informações sob responsabilidade das entidades preservando sua confidencialidade, integridade, disponibilidade e autenticidade;

III. Prevenir eventuais interrupções, totais ou parciais, dos serviços de TI acessados pelas entidades e pelos cooperados e, no caso de sua ocorrência, reduzir os impactos dela resultantes;

IV. Tratar e prevenir incidentes de segurança cibernética;

V. Formar e qualificar os recursos humanos necessários à área de segurança cibernética;

VI. Promover o intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética.

A COOPERATIVA DE CRÉDITO DOS MAGISTRADOS DO ESTADO DO RIO DE JANEIRO LTDA – MAGICREDI-RJ deve implementar e manter Política de Segurança Cibernética, conforme definições em princípios e diretrizes a seguir relacionados, de modo a assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Essa Política será compatível com os seguintes aspectos:

I. O porte da Cooperativa, que é classificada como "Cooperativa Clássica" pela Resolução BACEN 5.051/2022 (art. 2º alínea II), e classificada como perfil de risco ponderado na forma simplificada, por restrições de diversas operações, que não tem permissão para realizar;

II. A natureza de suas operações, não havendo complexidade dos produtos que pode operar por sua classificação; e,

III. A sensibilidade dos dados e das informações sob responsabilidade da Cooperativa.

A Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro - MAGICREDI-RJ não faz parte de nenhum Sistema Cooperativo de Crédito, sendo, portanto, considerada uma Cooperativa "**Solteira"** para o Banco Central do Brasil.

4. APLICAÇÃO

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos ativos disponibilizados pela cooperativa ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela cooperativa, sendo de responsabilidade individual e coletivo o seu cumprimento.

5. A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é uma importante aliada na prevenção e na recuperação de incidentes de segurança, definindo critérios, normas e procedimentos seguros para proteger os ativos da informação e garantir as propriedades básicas de segurança nos sistemas de informação.

Está baseada na proteção preventiva de toda a cadeia de dados confidenciais ou não processados, que são de responsabilidade da Cooperativa, e que são manuseados pelos membros estatutários ou colaboradores da Cooperativa, visando à plena confidencialidade desses dados nas diversas formas que são geradas, com ênfase no armazenamento cibernético.
Essa proteção preventiva requer controles e níveis de acesso às informações; a contínua vigilância e principalmente, sistemas adequados e confiáveis contratados para processamentos e armazenamentos de dados.

Os pilares da segurança da informação nos dão subsídios para proteger as informações da MAGICREDI-RJ. Portanto, quando mencionamos "segurança da informação" entende-se que estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como aos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa. (ISO 27002 A.5.1.1)

O que é Política de Segurança da Informação?

É um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável. (ISO 27002 A.5.1.1)

A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo.

Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a Cooperativa em locais públicos ou com pessoas estranhas ao nosso meio. (ISO 27002 A.5.1.1)

6. RESPONSABILIDADE NA GESTÃO DA POLÍTICA

A Cooperativa de Crédito dos Magistrados do Estado do Rio de Janeiro - MAGICREDI-RJ, Cooperativa singular, por meio da Diretoria Executiva, é responsável pelo gerenciamento da segurança cibernética na entidade que administram.

Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos e atender aos demais objetivos da Política de Segurança Cibernética, as entidades da MAGICREDI-RJ adotam procedimentos e controles, conforme porte e perfil de risco da entidade.

Estes procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

É estabelecido plano de ação e de resposta a incidentes, revisado anualmente.

As empresas terceirizadas que manuseiam dados ou informações sensíveis ou que são relevantes para a condução das atividades operacionais estabelecem procedimentos e controles compatíveis aos utilizados pelas entidades da MAGICREDI-RJ.

As informações de propriedade ou sob custódia da ***MAGICREDI-RJ***, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, conforme manual de classificação da informação específico.

São adotados mecanismos para disseminação da cultura de segurança cibernética na instituição.

Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a Política de Segurança Cibernética no âmbito da entidade da MAGICREDI-RJ.

6.1 Alta Administração

a) prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;
b) prover comprometimento e apoio à aderência a Política de Segurança Cibernética e da Informação de acordo com os objetivos e estratégias de negócio estabelecidas para organização;
c) fornecer à área responsável pela Segurança da Informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário;
d) identificar requisitos legais pertinentes a segurança da informação;
e) garantir a adoção de cláusulas pertinentes à segurança da informação nos contratos estabelecidos com a cooperativa.

6.2 Colaboradores:

a) cumprir fielmente esta Política;
b) buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Confidenciais;
c) proteger Informações Confidenciais contra acesso, modificação, destruição ou divulgação não autorizadas pela cooperativa;
d) assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela cooperativa;
e) cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Confidenciais;
f) comunicar imediatamente à diretoria sobre qualquer descumprimento ou violação desta Política;
g) utilizar de modo seguro, responsável, moral e ético todos os serviços e sistemas de TI;
h) notificar ao responsável de TI sobre as violações da Política de Segurança Cibernética e da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;
i) manter o sigilo das informações que tenha obtido acesso enquanto Colaborador da

cooperativa, mesmo após seu desligamento da empresa.

6.3 – Gestor

a) Apoiar e incentivar o estabelecimento da Política de Segurança Cibernética e da Informação na Cooperativa;
b) garantir que seus subordinados tenham acesso e conhecimento desta Política e demais normas e padrões de segurança da informação;
c) fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da cooperativa;
d) avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
e) 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;
f) acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem a Política de Segurança Cibernética e da Informação e as normas da Cooperativa;
g) autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de *need to know* e *least privilegie*.

6.4 Área de Infraestrutura

a) orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
b) desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança Cibernética e da Informação;
c) conduzir o processo de Gestão de Riscos de Segurança da Informação;
d) conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis, bem como a comunicação dos fatos ocorridos;
e) conduzir os processos de monitoramento e segurança da informação;
f) definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
g) propor projetos e iniciativas para melhoria do nível de segurança das informações da MAGICREDI-RJ;
h) manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de *hardware* e *software*;
i) tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
j) conduzir a gestão dos acessos a sistemas e informações da MAGICREDI-RJ;
k) implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
l) informar imediatamente a alta direção, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da MAGICREDI-RJ;
m) controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;

n) garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio;
o) garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como *Datacenters*. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

6.5 Fornecedores e Parceiros de Negócios

a) cumprir as determinações da Política, Normas e Procedimentos publicados pela MAGICREDI-RJ;
b) orientar os funcionários da empresa sobre o cumprimento das determinações da Política, Normas e Procedimentos publicados pela MAGICREDI-RJ;
c) cumprir com o acordo de confidencialidade.

6.6 Penalidades

O colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração ao responsável pela Infraestrutura. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

No caso de prestadores de serviços terceirizados, pode ser solicitada às suas respectivas empresas a troca da equipe alocada na MAGICREDI-RJ, ou ainda, podem ser aplicadas penalidades a empresa tais como multas, cancelamento do contrato e ações judiciais.

7. CONCEITOS E PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Todas as Informações Confidenciais constituem ativos de valor para a MAGICREDI-RJ e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Cooperativa, Cooperados e Colaboradores.

As Informações Confidenciais podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos e mensagens eletrônicas, sites de *Internet*, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Confidenciais deve ser prioridade constante da cooperativa, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a sua imagem e objetivos. Assim, por princípio, a guarda e segurança das Informações Confidenciais deve abranger três aspectos básicos, destacados a seguir:

a) **acesso**: somente pessoas devidamente autorizadas pela cooperativa devem ter acesso às Informações Confidenciais;

b) **integridade**: somente alterações, supressões e adições autorizadas pela cooperativa

devem ser realizadas às Informações Confidenciais;

c) **disponibilidade**: as Informações Confidenciais devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado; e

d) **confidencialidade**: Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntária ou involuntariamente, dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

Para assegurar os 04 (quatro) aspectos acima, as Informações Confidenciais devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em cumprimento à Resolução nº 4.893/21, a cooperativa possui 4 (quatro) pilares principais no seu programa de segurança cibernética:

a) identificação e avaliação de riscos (*risk assessment*);
b) ações de prevenção e proteção;
c) monitoramento e testes; e
d) plano de resposta.

A implantação e monitoramento da capacidade da cooperativa que atender a estes pilares deverá ser feito pelo Diretor responsável. Também a fim de atingir os objetivos dispostos acima, cada setor da cooperativa terá suas próprias responsabilidades.

A cooperativa deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação da Diretoria promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de Informações Confidenciais, para que possam agir de maneira apropriada frente as situações que requeiram respostas.

Além disso, ainda conforme está previsto na Resolução 4.893/2021, devem ser previstos diversos aspectos da segurança cibernética e que irão nortear essa política:

I. Objetivos da Politica de Segurança Cibernética - assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados;

II. Procedimentos e os controles adotados para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos objetivos da Política de Segurança Cibernética - Esses procedimentos requer controles e níveis de acesso às informações; a contínua vigilância e principalmente, sistemas adequados e confiáveis contratados para processamentos e armazenamentos de dados;

III. Controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis - Esses procedimentos requer a utilização de equipamentos e programas confiáveis, com a utilização de programas de antivírus adequados e capazes de assegurar a confiabilidade da proteção, aliado a uma manutenção preventiva e

constante dessas ferramentas. O armazenamento em nuvem deverá ser adotado como princípio de segurança confiável;

IV. O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição - Deve-se estar atento às tentativas de ataques cibernéticos, bem como as apurações em casos de incidentes relevantes ou não, pois qualquer ocorrência demonstrará falhas nas defesas ou prevenções, devendo ser debatidas as ocorrências nos diversos níveis operacionais da Cooperativa, buscando aprimoramento dos mecanismos preventivos;

V. As diretrizes para:

a) A elaboração de cenários de incidentes considerados nos testes de continuidade de negócios - Deve-se levar em consideração cenários que possam abalar os negócios, causando interrupções danosas às operações; acesso e roubos de informações confidenciais; acesso e roubos nas contas de depósitos da Cooperativa; destruição de arquivos e bancos de dados; bloqueio de acessos com a liberação mediante resgates criminosos, entre outros;

b) A Definição de procedimentos e de controles voltados à prevenção e ao tratamento de incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que seja relevante para a condução das atividades operacionais da Cooperativa - Trata-se de uma parte extremamente relevante na política de segurança cibernética, pois a relação cooperativa e as empresas prestadoras desses serviços deve estar estruturada além da sua capacitação técnica, na confiabilidade recíproca conquistada em anos de relacionamento. Juridicamente deve estar ancorada em contrato, que seja considerado um ato jurídico perfeito, com cláusulas pétreas e preventivas de segurança, além dos aspectos técnicos sobre os serviços contratados e outros, devendo ser revisto periodicamente para atualizações, aperfeiçoando essa relação com uma segurança jurídica garantidora da prestação dos serviços;

c) A classificação dos dados e das informações quanto à relevância - A Cooperativa como instituição financeira, opera com informações protegidas por sigilo de acordo com a Legislação em vigor (Lei Complementar 105/2001), que relaciona essas operações cuja violação é passível de penalizações. Essas operações elencadas terão tratamento prioritário na classificação de dados na política de segurança cibernética tanto pela relevância, quanto pela penalização imposta por sua violação. O seu manuseio e acesso pelas pessoas que por dever de ofício tem autorização para fazê-lo, deverão ser cientificadas quanto a violações. Outros tipos de dados e informações poderão ter classificação mais abrandada nas atividades da cooperativa;

d) A definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes - Como está evidenciado no item “c” anterior, os parâmetros levarão em consideração em primeiro lugar, as informações previstas na Lei Complementar 105/2001 e que a cooperativa por sua classificação está

autorizada a operar. Atendida essa relevância, as demais informações serão avalizadas por outros critérios, dentro das relevâncias julgadas pertinentes.

VI. Os mecanismos de disseminação da cultura de segurança cibernética na cooperativa, incluindo:

a) A implementação de programas de capacitação e de avaliação periódica de pessoal – Dentro dos programas de treinamento e capacitação dos membros estatutários e colaboradores, a cooperativa incluirá a Segurança Cibernética como programa de capacitação, bem como a avaliação do pessoal;

b) A prestação de informações a clientes e usuários sobre precaução na utilização de produtos e serviços financeiros - Essa é uma parte sensível no relacionamento cooperativa e seus associados, pois a cooperativa apesar de sua classificação como **"CLÁSSICA"**, centrando suas operações na captação de recursos e empréstimos, não pode negligenciar nas orientações e precauções na utilização desses serviços. Os colaboradores serão orientados sempre na prestação dos atendimentos e a informações e orientações no trato desses serviços, que são protegidos pelo sigilo previsto na Lei Complementar 105/2001;

c) O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a Segurança Cibernética - A Diretoria da Cooperativa deverá ter comprometimento prioritário com a Segurança Cibernética, pois além de ter um diretor responsável pela segurança indicado, deverá buscar estar inteirada no que ocorre na área de Segurança Cibernética, atuando preventivamente, cobrando informações e providências diuturnas.

VII. As iniciativas para compartilhamento de informações sobre incidentes relevantes mencionados no inciso IV, com outras Cooperativas de Crédito - Trata-se de uma prática que não é comum, mas que deve ser buscada em função de que diversos incidentes são comuns tendo como origem fontes idênticas e o mesmo "modus operandi". Uma das formas seria através das empresas de informática contratadas, e que prestam serviços a diversas cooperativas e serviriam de elo de compartilhamento de incidentes, e que para tanto, deveriam ser autorizadas a divulgarem incidentes ocorridos para ações preventivas.

Considerações complementares sobre os incisos citados anteriormente:

Inciso I – Deverá ser contemplada a capacidade da Cooperativa para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, situação esta que está ligada aos operadores do sistema de informática (equipamentos e programas), com sistemas adequados de detecção.

Inciso II – Os procedimentos e controles devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção da vulnerabilidade, a proteção contra programas maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações,

devendo também ser aplicado, no desenvolvimento ou contratação de sistemas de informação seguros, e na adoção de novas tecnologias empregadas na atividade da cooperativa.

Inciso III – O registro, a análise da causa e o impacto, bem como o controle dos efeitos de incidentes, devem abranger inclusive informações recebidas das empresas de prestação de serviços de informática contratadas.

Inciso IV – As diretrizes devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela cooperativa.

8. PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A Cooperativa estabelecerá Plano de Ação e de Resposta a Incidentes que é parte integrante da Política de Segurança Cibernética.

Este Plano abrangerá o seguinte:

I. Ações a serem desenvolvidas pela Cooperativa para adequar sua estrutura organizacional e operacional aos princípios e às diretrizes de segurança cibernética prevista;

II. As rotinas, os procedimentos, os controles e as tecnologias que serão utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança prevista;

III. A área responsável pelo registro e controle dos efeitos de incidentes relevantes que terá um diretor responsável pela Política de Segurança Cibernética, a ser informado ao BACEN através do **UNICAD**.

9. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM.

A Resolução BACEN 4.893/2021 prevê que as instituições financeiras devem assegurar que suas políticas estratégicas e estruturas para gerenciamento de riscos de segurança cibernética, devem levar em consideração os critérios de decisão quanto à terceirização na contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, tanto no país e/ou no exterior. Para contratação desses serviços, previamente devem ser adotados os seguintes procedimentos:

I. A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;

II. A verificação da capacidade no potencial do prestador de serviços para assegurar o cumprimento da legislação e da regulamentação em vigor; o acesso da cooperativa aos dados e às informações a serem processados ou armazenados pelo prestador de serviços; a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviços; sua aderência a certificações exigidas; o acesso da cooperativa aos relatórios gerados pelas auditorias independente do prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados; o provimento de informações e de

recursos de gestão adequados no monitoramento dos serviços a serem prestados; identificação e segregação dos dados dos clientes da cooperativa por meio de controles físicos ou lógicos e a qualidade dos controles de acesso voltados à proteção dos dados e das informações.

Estamos contratando os serviços de armazenamento de dados e de computação em nuvem – Sistema FACCRED, versão SaaS, da empresa REZEK FERREIRA INFORMÁTICA LTDA, nome fantasia Fácil Informática, sediada na Rua Ouro Preto, nº 1.668, 6º andar, no bairro Stº Agostinho, CEP 30.170-048, na cidade de Belo Horizonte, Estado de Minas Gerais, inscrita no CNPJ sob o nº 00.881.775/0001-13. O pacote contempla todos os serviços relacionados à utilização do FACCERD, versão SaaS – *software* como serviço. As aplicações ficam hospedadas em servidores de alta disponibilidade na nuvem AMAZON *Web Services*.

O serviço viabiliza a execução de todos os módulos licenciados do sistema Fácil Informática, sem a necessidade de instalação de *software* na estação cliente. No novo modelo de uso, não será mais necessário à instalação e licenças de servidores locais, incluindo banco de dados. O serviço de *backup* em nuvem será totalmente automatizado, em ambiente de alta disponibilidade e durabilidade, com garantia da integridade dos dados através de restaurações periódicas em ambiente de homologação. Acompanhamento de DBA especializado nos sistemas ERP da Fácil Informática, contemplando desde o dimensionamento, instalação e configuração até *tuning*, *backup/recover*, monitoramento e aplicação de *patches*. Monitoramento de servidores e serviços com notificação via *e-mail*, SMS, Twiter em caso de falhas. Possui características pró-ativas (ações para antecipação de falhas), re-ativas (ações de resposta e eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas). Visando melhor exemplificar os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, anexo cópia da proposta de serviço firmado com a Fácil Informática.

A AMAZON *Web Service*, através de sumário anexo, fornece um guia de informações que buscam evidenciar suas certificações, sua base nos EUA, país com acordo para troca de informações entre BACEN e as autoridades locais, bem como atender o solicitado nos demais itens do artigo 16º da Resolução 4.893/21.

As políticas da Amazon de segurança **Compliance** e SLA podem ser acessadas nos seguintes links:

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
https://aws.amazon.com/pt/compliance/programs/
https://d1.awsstatic.com/legal/amazon-ec2-sla/Amazon_EC2_Service_Level_Agreement_-_Portuguese_Translation__2018-02-12_.pdf

10. PLANO DE CONTINUIDADE DE NEGÓCIOS

A resolução do BCB exige que as IFs tenham um Plano de Continuidade de Negócios que inclua determinados elementos. Por exemplo, o capítulo III, seção 16.IV, exige que a IF defina alternativas para o uso de um provedor de serviços em nuvem para continuidade de

negócios no caso de impossibilidade de manutenção ou término do contrato de serviços. Além disso, as seções 19 e 20 do capítulo IV exigem que a IF tenha políticas de gerenciamento de riscos que abordem a continuidade de negócios e as respostas a incidentes relevantes.

O Plano de Continuidade de Negócios da Cooperativa destinou a AWS detalhar o processo que segue no caso de uma interrupção, desde a detecção até a desativação. Este plano foi desenvolvido para recuperar e reconstituir a AWS usando uma abordagem de três fases: Fase de Ativação e Notificação, fase de Recuperação e fase de Reconstituição.

Essa abordagem garante que a AWS realize os procedimentos de recuperação e reconstituição do sistema em uma sequência metódica, maximizando a eficácia dos esforços de recuperação e reconstituição e minimizando o tempo de interrupção do sistema devido a erros e omissões.

A AWS mantém um ambiente de controle de segurança onipresente em todas as regiões. Os clientes usam a AWS para alcançar uma recuperação de desastres mais rápida em seus sistemas de TI críticos, sem incorrer em gastos de infraestrutura de um segundo site.

A Nuvem AWS oferece suporte a muitas arquiteturas populares de recuperação de desastres (DR), desde ambientes de "*pilot light*", que estão prontos para serem escalados a qualquer momento, até ambientes de "*hot standby*", que permitem um *failover* rápido.

Os clientes podem encontrar mais informações sobre como arquitetar um DR na Nuvem AWS aqui: https://aws.amazon.com/pt/disaster-recovery/

11. REGRAS DE USO DOS RECURSOS DE TECNOLOGIA

- Os recursos tecnológicos que são de propriedade da Cooperativa são autorizados e disponibilizados exclusivamente para os usuários desempenharem suas funções a serviço da Cooperativa;
- A comunicação através dos recursos tecnológicos deve ser formal e profissional dentro da ética, de modo a preservar a imagem institucional da Cooperativa;
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia devem ser legais, bem como a utilização de equipamentos e programas, de modo a contribuir para atividades profissionais dentro da ética;
- O uso dos recursos de tecnologia deverá ser submetido a testes periódicos pela Auditoria Interna, com pleno conhecimento e autorização da Diretoria da Cooperativa, e em conformidade com a Resolução BACEN 4.8936/2021.
- Cada usuário é responsável pelo uso dos recursos tecnológicos que lhe for confiado e autorizado, que estarão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas instalados, sendo vedado o uso de programas ilegais nos equipamentos;
- Os recursos de tecnologia da Cooperativa disponibilizados para os usuários, não podem ser repassados para terceiros estranhos à cooperativa, salvo em caso de autorização expressa.

- Qualquer anormalidade ou irregularidade nos recursos de tecnologia devem ser comunicados de imediato aos superiores hierárquicos.

12. REGRAS A SEREM CUMPRIDAS PARA UTILIZAÇÃO DOS MEIOS TECNOLÓGICOS E DE COMUNICAÇÃO

12.1 USO DO COMPUTADOR

- Os computadores disponibilizados para o usuário são de propriedade da Cooperativa, e deve(m) ser utilizado(s) com zelo e os cuidados necessários para assegurar seu(s) pleno (s) funcionamento dentro da vida útil estimada de uso(s);
- O computador é uma ferramenta tecnológica disponibilizada para o usuário, que tem como objetivo facilitar o desempenho de suas atividades profissionais, com o pressuposto do usuário possuir capacitação técnica para utilizar a ferramenta;
- A utilização do(s) equipamento(s) poderá implicar e/ou exigir a utilização de senha específica e login de acesso, bem como limites de acesso, de modo a que se possa identificar a qualquer tempo o usuário na realização de tarefas, pois a senha e o *login* serão a assinatura digital do usuário;
- A cooperativa pode a qualquer tempo suspender, limitar e/ou proibir o acesso de usuário, em casos supervenientes que justifiquem;
- É vedada a cessão de senha pelo usuário, sendo de sua inteira responsabilidade tal ocorrência, pois a mesma é pessoal e intransferível;
- Será exigido que num prazo de 180 dias as senhas sejam trocadas, podendo ocorrer a qualquer momento pelo usuário ou superior hierárquico;
- Os programas básicos, operacionais e aplicativos instalados no(s) computador (res) são de responsabilidade da cooperativa, cabendo ao usuário a sua correta utilização, desde que esteja capacitado para tal, e em caso de necessidades, deverá encaminhar solicitação ao superior hierárquico de novas configurações;
- O usuário tem a responsabilidade de cuidar adequadamente do(s) equipamento(s) que utiliza, sendo considerado o custodiante desses recursos, garantindo a sua integridade física, seu funcionamento, bem como solicitação de manutenção;
- Bloqueios de acesso podem ser implantados como formas preventivas de incidentes, devendo o usuário estar sempre atento a atualizações de programas de proteção antivírus; tentativas de ataques; programas maliciosos e outras situações que possam redundar em incidentes, devendo estar também sempre atento a realizar cópias de segurança de programas e arquivos, se for de sua responsabilidade, evitando negligências como não realizar cópias nos períodos determinados; armazenar em locais seguros, mesmo que faça arquivamento de dados em nuvem; não deixar cópias de segurança acopladas a equipamentos, pois em caso de ataques as perdas custarão caro;

- O usuário deve estar ciente que a instalação ou utilização de programas não autorizados, constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19.02.1998, sujeitando os infratores a pena de detenção e multa. A cooperativa não se responsabiliza por qualquer ação individual que esteja em desacordo com a lei mencionada, sendo considerada sua prática uma ameaça à segurança da informação, e será tratada com aplicação de ações disciplinares.

10.2 USO DA INTERNET

- O usuário é responsável por todo acesso realizado com sua autenticação;
- Não é permitido ao usuário acessar endereços na *Internet* que possam violar direitos de autor; marcas; licenças de programas ou patentes existentes registradas; conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia; contenham informações que não colaborem ou prejudiquem para o alcance dos objetivos da Cooperativa; defendam atividades ilegais; menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;
- O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes, e que o uso do material foi autorizado pelo gestor de sua área;
- O uso de serviços tais como mensagens instantâneas; uso de serviço de rádio, TV, *download* de vídeos, filmes, músicas, e correio eletrônico particular, poderão ser toleradas suas utilizações pelo usuário, desde que não se confunda e nem prejudiquem os trabalhos da Cooperativa, situação que poderá não ser permitida e até proibida.

10.3 USO DO CORREIO ELETRÔNICO

- A cooperativa disponibiliza endereços de seu correio eletrônico para utilização dos usuários, no desempenho de suas funções profissionais, que pode ser o geral da MAGICREDI-RJ, como também específico para o usuário, desde que simplifique e agilize os trabalhos a realizar;
- No caso de endereço eletrônico individual para usuário, este é intransferível e pertence à cooperativa, sendo o mesmo enquanto permanecer o vínculo com a Cooperativa;
- Em caso de necessidade por qualquer que seja o motivo justificado e aprovado, poderá haver alteração no endereço individual;
- O usuário que utiliza o endereço individual do correio eletrônico da cooperativa é responsável por todo o acesso, conteúdo de mensagens e uso relativo ao seu *e-mail*, podendo enviar mensagens necessárias ao seu desempenho profissional e a sua atuação na Cooperativa;
- Não é permitido criar, copiar ou encaminhar mensagens ou imagens que contenham declarações difamatórias ou linguagem ofensiva de qualquer

natureza; façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;

- O usuário deve estar ciente que o correio eletrônico da cooperativa deve ser utilizado para os serviços da instituição em todos os seus aspectos formais e profissionais, devendo abster-se de uso particular ou em benefício de terceiros não autorizados, salvo se previamente autorizado;

- O uso indevido do correio eletrônico da cooperativa será passível de sanções disciplinares, principalmente por tratar-se de uma forma de comunicação sensível para a imagem da cooperativa como instituição financeira, não devendo ser exposta de maneira inadequada por essa poderosa ferramenta de comunicação, até por causa das implicações legais dessas mensagens, sendo até utilizadas como provas em juízo em casos de contendas.

10.4 USO DO TELEFONE

- A Cooperativa disponibiliza telefone(s) fixo(s) para utilização dos membros estatutários e usuários colaboradores, para atendimento ao quadro social e ao público em geral;
- O telefone como meio de comunicação, é parte fundamental da segurança da informação da cooperativa;
- Sua utilização fundamental é ser um canal de comunicação entre a cooperativa e seus associados, sendo prioritário o seu funcionamento nessa tarefa;
- O usuário colaborador deve saber que esse tipo de comunicação alavanca as atividades da cooperativa, e por isso deve ser utilizado de forma ética e profissional no trato com sua clientela, e que são os seus cooperados;
- Os atendimentos devem ser formais e objetivos aos usuários clientes, fornecedores e ao público em geral, de modo que fique evidenciado um padrão de atendimento que será uma das marcas da cooperativa para esse público;
- O usuário colaborador deve ser breve e objetivo, sendo que nos casos em que não consiga dar o atendimento adequado, deve dirigir ao superior hierárquico sua solução;
- O usuário colaborador pode receber e fazer chamadas particulares, mas sempre com brevidade e objetividade, de modo que a(s) linha(s) estejam prontamente liberadas o mais rápido possível para atendimento do público usuário;
- O uso racional das linhas telefônicas pressupõe economia no custo mensal com telefone, devendo ser buscado e implementado por todos;
- O usuário colaborador deverá estar sempre atento em evitar prestar informações confidenciais no telefone ao quadro social, uma vez que pode não ser a pessoa do outro lado da linha, a não ser que pela prática, tenha a plena certeza que trata-se do associado certo e que busca informações,

principalmente as confidenciais. Via de regra, as informações confidenciais devem ser prestadas presencialmente, ou através de sistemas confiáveis. Nunca é demais lembrar que o vazamento de informações confidenciais, são passíveis de punições por força da Lei Complementar 105/2001.

11 LINHAS GERAIS DO COMPORTAMENTO SEGURO

- O usuário colaborador deve saber que o acesso à cooperativa é vedado para aqueles que não são membros estatutários e usuários colaboradores e/ou prestadores de serviços. O acesso quando ocorrer para quem é vedado, deve ser sob expressa autorização e de forma limitada. Os dados confidenciais não podem ser acessados de maneira alguma para quem não é permitido. O atendimento ao quadro social e ao público em geral, deve ser de forma destacada, e de preferência, sem acesso ao local de trabalho da equipe;
- O usuário colaborador deve ter sempre o devido cuidado no ambiente externo da cooperativa, evitando falar informações restritas e confidenciais, como também em portar "*laptops* ou *pendrives*" com informações confidenciais;
- O usuário colaborador deve ter o devido cuidado com o lixo de informações confidenciais. Deve-se procurar utilizar fragmentadoras de papéis para o correto descarte desses documentos;
- O usuário colaborador deve ter o devido e imprescindível cuidado com suas senhas e *logins* de acesso aos equipamentos, pois eles são suas assinaturas digitais, e a sua violação pode gerar enormes prejuízos à cooperativa, e punições serão inevitáveis, que poderão ser no mínimo por negligência;
- O usuário colaborador deverá adotar um comportamento seguro quanto a não compartilhar e nem divulgar sua senha a terceiros; não transportar informações confidenciais sem o conhecimento e/ou a devida autorização; não discutir assuntos confidenciais em ambiente público; abrir *e-mails* com mensagens de origem desconhecida ou suspeita; armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos com informações confidenciais, e por fim, seguir corretamente a política de segurança cibernética para uso da *Internet* e correio eletrônico, ou outras formas de comunicação, como aplicativos *site*; *Whatsapp*; *Facebook*; *Instagram* e outros, caso sejam utilizados pela Cooperativa.

13. REVISÕES E ATUALIZAÇÕES

De acordo com o art. 10, da Resolução nº 4.893/21, esta Política será revisada pelo menos uma vez a cada ano. Não obstante as revisões estipuladas poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

14. VIGÊNCIA

Esta Política de Segurança Cibernética foi aprovada em Reunião da Diretoria Executiva da COOPERATIVA DE CRÉDITO DOS MAGISTRADOS DO ESTADO DO RIO DE JANEIRO LTDA-MAGICREDI-RJ, em 25 de agosto de 2023 e passa a vigorar na data de sua aprovação devendo ser divulgada no *site* para todos os membros estatutários; aos usuários, colaboradores, prestadores de serviços bem como ao quadro social.

Rio de Janeiro, 23 de agosto de 2023.

ADEMIR PAULO PIMENTEL:10440569753
Assinado de forma digital por ADEMIR PAULO PIMENTEL:10440569753
Dados: 2024.06.06 16:09:57 -03'00'

ADEMIR PAULO PIMENTEL
DIRETOR PRESIDENTE

NILTON RAMOS DANTAS SANTOS
DIRETOR SECRETÁRIO