COOPMAUA

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

COOPMAUA

PREÂMBULO

A COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS FUNCIONÁRIOS DO GRUPO MAUÁ E EMPRESAS COLIGADAS LTDA. – COOPMAUÁ, considerando a natureza de suas atividades, seu porte, perfil de risco, modelo de negócio, complexidade de suas operações e a sensibilidade dos dados e informações sob sua responsabilidade, estabelece a presente Política de Segurança Cibernética e da Informação.

Esta Política tem por finalidade estabelecer os princípios, diretrizes e responsabilidades destinados a assegurar a confidencialidade, a integridade, a disponibilidade e a segurança dos dados, das informações, dos sistemas e dos recursos tecnológicos utilizados pela Cooperativa, bem como orientar a adoção de procedimentos e controles voltados à prevenção, detecção, resposta e mitigação de incidentes relacionados ao ambiente cibernético.

A presente Política observa as disposições da Resolução CMN nº 4.893, de 26 de fevereiro de 2021, e suas alterações posteriores, especialmente as promovidas pela Resolução CMN nº 5.274, de 18 de dezembro de 2025, considerando os requisitos aplicáveis à implementação e manutenção da estrutura de segurança cibernética pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

A COOPMAUÁ adotará procedimentos e controles compatíveis com sua estrutura, perfil de risco e realidade operacional, destinados à proteção de seus ativos de informação e à redução de vulnerabilidades relacionadas ao ambiente tecnológico, observando os requisitos regulatórios aplicáveis e a proporcionalidade necessária à sua natureza e complexidade operacional.

Esta Política também estabelece diretrizes gerais relacionadas à proteção das informações e dos dados pessoais tratados pela Cooperativa, reconhecendo que a segurança cibernética constitui importante instrumento para prevenção de acessos não autorizados, perdas, vazamentos, alterações indevidas e demais incidentes que possam comprometer informações sob sua responsabilidade.

As diretrizes aqui estabelecidas deverão ser observadas pelos administradores, colaboradores e, quando aplicável, prestadores de serviços que tenham acesso às informações, sistemas ou recursos tecnológicos da COOPMAUÁ.

REFERÊNCIAS NORMATIVAS

A presente Política observa, entre outras aplicáveis:

- Resolução CMN nº 4.893/2021;
- Resolução CMN nº 5.274/2025, que alterou a Resolução CMN nº 4.893/2021;

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;
- Resolução CD/ANPD nº 15/2024 – Regulamento de Comunicação de Incidente de Segurança;
- Demais normas do Conselho Monetário Nacional, Banco Central do Brasil e Autoridade Nacional de Proteção de Dados aplicáveis à COOPMAUÁ.

Esta Política está dividida nas seguintes seções:

1 - Do Objeto e do Âmbito de Aplicação

2 - Importância da Segurança da Informação

3 - Princípios da Segurança da Informação

4 - Plano de Ação e de Resposta a Incidentes

4.1 - Regras do Uso dos Recursos de Tecnologia

4.2 - Regras para o Uso do Computador

4.3 - Regras para o Uso da Internet

4.4 - Regras para Uso do Correio Eletrônico

4.5 - Regras para Uso do Telefone

4.6 - Linhas Gerais do Comportamento Seguro

5 - Contratação de serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem.

COOPMAUA

1 – DO OBJETO E DO ÂMBITO DE APLICAÇÃO

A COOPMAUÁ deve implementar e manter Política de Segurança Cibernética e da Informação, formulada com base em princípios e diretrizes destinados a assegurar a confidencialidade, a integridade e a disponibilidade dos dados, das informações e dos sistemas utilizados pela Cooperativa.

A presente Política deverá ser compatível com:

I – o porte, o perfil de risco e o modelo de negócio da Cooperativa;

II – a natureza das operações e a complexidade dos produtos, serviços, atividades e processos desenvolvidos; e

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

A COOPMAUÁ não faz parte de nenhum Sistema Cooperativo de Crédito, sendo portanto considerada, uma Cooperativa "Independente" para o Banco Central do Brasil, sendo filiada à Federação Nacional das Cooperativas de Crédito Urbano - FENACRED.

2 – A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

A importância 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 gerados, 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.

A segurança da informação constitui elemento essencial para a proteção dos ativos informacionais da COOPMAUÁ, abrangendo informações em meio físico ou digital, sistemas, equipamentos, documentos, bases de dados e demais recursos utilizados no desenvolvimento de suas atividades.

A proteção das informações deverá observar medidas compatíveis com sua relevância e sensibilidade, buscando prevenir acessos não autorizados, perdas, alterações indevidas, vazamentos, indisponibilidade ou qualquer outra situação que possa comprometer a confidencialidade, a integridade ou a disponibilidade das informações.

3 – PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Conforme está previsto na Resolução, devem ser previstos diversos aspectos da segurança cibernética e que irão nortear essa política:

Os objetivos de segurança cibernética deverão contemplar também a capacidade da COOPMAUÁ para prevenir, detectar e reduzir sua vulnerabilidade a incidentes relacionados ao ambiente cibernético.

Os procedimentos e os controles adotados para reduzir a vulnerabilidade da COOPMAUÁ a incidentes e atender aos demais objetivos de segurança cibernética devem abranger, no mínimo:

I – a autenticação;

II – os mecanismos de criptografia;

III – os mecanismos de prevenção e detecção de intrusão;

IV – os mecanismos de prevenção de vazamentos de informações;

V – os mecanismos de proteção contra softwares maliciosos;

VI – os mecanismos de rastreabilidade;

VII – a gestão de cópias de segurança dos dados e das informações;

VIII – a avaliação e a correção de vulnerabilidades dos recursos computacionais e dos sistemas de informação;

IX – os controles de acesso;

X – a definição e implementação de perfis de configuração segura de ativos de tecnologia;

XI – os mecanismos de proteção da rede;

XII – a gestão dos certificados e assinaturas digitais utilizados pela COOPMAUÁ deverá observar controles destinados ao monitoramento de sua utilização, à proteção das credenciais e chaves privadas sob responsabilidade da Cooperativa, à prevenção de compartilhamento indevido e ao acompanhamento de sua validade e situação perante as autoridades certificadoras, quando aplicável;

XIII – os requisitos de segurança para a integração de sistemas de informação por meio de interfaces eletrônicas; e

XIV – as ações de inteligência no ambiente cibernético, incluindo o monitoramento de informações de interesse da Cooperativa na internet e, quando aplicável, em ambientes restritos ou especializados de informação.

§ 1º Os procedimentos e os controles citados neste inciso devem ser aplicados, inclusive:

I – no desenvolvimento de sistemas de informação seguros; e

II – na adoção de novas tecnologias empregadas nas atividades da COOPMAUÁ.

III – Controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis. Esses procedimentos requerem a utilização de equipamentos e programas confiáveis, com a utilização de programas 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. Os mecanismos de rastreabilidade deverão contemplar, de forma compatível com os sistemas e operações da COOPMAUÁ, trilhas de auditoria e registros que permitam identificar falhas de processamento, comportamentos atípicos e eventos relevantes, bem como a definição de critérios para retenção e guarda segura desses registros.

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 entre aCooperativa 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 estão evidenciados 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 "capital e empréstimo", centrando suas operações nessas duas modalidades, 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 previstos 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.

4 – PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES.

A COOPMAUÁ deverá realizar, de forma compatível com sua estrutura e riscos, testes, varreduras e análises periódicas destinadas à identificação de vulnerabilidades em seus recursos tecnológicos e sistemas de informação, adotando medidas para o tratamento e correção tempestiva das vulnerabilidades identificadas. Os testes de intrusão deverão observar a periodicidade mínima e os requisitos de independência, documentação dos resultados e estabelecimento de planos de ação previstos na regulamentação vigente.

Este Plano abrangerá o seguinte:

1) Ações a serem desenvolvidas pela Cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes de segurança cibernética previstas.

2) 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.

3) A área responsável pelo registro e controle dos efeitos de incidentes relevantes, que estará afeta ao diretor responsável designado pela Política de Segurança Cibernética, a ser informado ao BACEN através do UNICAD.

4) Conforme previsto na norma vigente, a cooperativa deverá apresentar relatório anual sobre a implementação de plano de ação e de resposta a incidentes descritos, com data base de 31 de dezembro de cada ano, e apresentado à diretoria até 31 de março do ano seguinte ao da data base, pelo diretor responsável designado.

5) O relatório deverá abordar, no mínimo, os seguintes tópicos:

I – a efetividade da implementação das ações descritas;

II – o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e resposta a incidentes;

III – os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV – os resultados dos testes de continuidade de negócios considerando cenários de indisponibilidade ocasionados por incidentes.

V – os resultados dos testes de intrusão e dos testes, varreduras e análises periódicas para detecção de vulnerabilidades, bem como os planos de ação estabelecidos para as respectivas correções, quando aplicáveis.

5 – 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 desegurança 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.

Previamente à contratação desses serviços, deverão ser adotados procedimentos que:

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 do potencial prestador de serviços de 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.

III – Deverão ser observados os aspectos previstos Capítulo III – ARTIGOS11 A 18 da Resolução 4.893/21, que trata da contratação dos serviços de processamento e armazenamento de dados e de computação em nuvem, com relação ao gerenciamento dos riscos previstos, avaliação da relevância do serviço a ser contratados, controles de utilização do uso de aplicativos, dos serviços disponibilizados, da segurança e do sigilo dos serviços contratados, da comunicação da contratação dos serviços, da contratação de serviços no exterior, etc.

DO SERVIÇO CONTRATADO

A Cooperativa tem contrato de Prestação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem com a Empresa:Prodaf Informática Ltda. - CNPJ nº 02.915.447/0001-16 - com sede na Avenida Waldemar

Mees, nº 42, andar2, sala 302, Centro, Marechal Floriano, Vitória/ES, CEP 29255-000, conforme cópia anexa e que faz parte dessa Política de Segurança Cibernética, firmado em 27 de abril de 2021.

REGRAS DE USO DOS SERVIÇOS SUJEITOS À SEGURANÇA CIBERNÉTICA

Regras do Uso dos Recursos de Tecnologia

A COOPMAUÁ deverá adotar mecanismos de proteção da rede compatíveis com sua estrutura tecnológica, contemplando controles destinados à prevenção de acessos e conexões indevidas, monitoramento de conexões, utilização de mecanismos de proteção adequados e restrição do acesso à rede corporativa a dispositivos devidamente autorizados.

. 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.

. Os recursos de tecnologia e os controles de segurança deverão ser submetidos a avaliações e testes periódicos, compatíveis com os riscos e com as requisitações regulamentares aplicáveis observada a independência das atividades de auditoria interna.

. 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.

COOPMAUA

Regras do Uso do Computador

. O (s) computador (res) disponibilizado(s) para o usuário é de propriedade da cooperativa, é 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 temcomo 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 loginserão 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 a superior hierárquico de novas configurações.

. Os recursos computacionais utilizados pela COOPMAUÁ deverão observar perfis de configuração segura, compatíveis com sua utilização e com os riscos envolvidos, contemplando, quando aplicável, a gestão do ciclo de vida dos recursos tecnológicos, a aplicação regular de correções de segurança, a configuração adequada dos serviços e a alteração de senhas e demais padrões que possam possibilitar acessos indevidos.

. 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.

. Os controles de acesso deverão contemplar mecanismos para limitar o acesso aos recursos tecnológicos e à rede corporativa a usuários credenciados e dispositivos autorizados, bem como a revisão periódica e tempestiva das permissões concedidas, especialmente nos casos de alteração de função, desligamento ou acesso por prestadores de serviços. Os acessos externos deverão observar mecanismos adicionais de autenticação, compatíveis com os riscos envolvidos.

Regras do 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 tolerados 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.

Regras do 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 cooperativa – coopmaua@coopmaua.com.br, 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.

Regras do Uso do Telefone

. A cooperativa disponibiliza telefone móvel para utilização dos membros estatutários e usuários colaboradores, para atendimento ao quadro social e ao público m 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 associados.

. Os atendimentos devem ser formais e objetivos aos usuários clientes, fornecedores e ao público em geral, de modo a 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 linha esteja prontamente liberada o mais rápido possível para atendimento do público usuário.

. O uso racional da linha telefônica 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 se trata 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, épassível de punições por força da Lei Complementar 105/2001.

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 Whatsapp; Facebook; Instagram e outros, caso sejam utilizados pela cooperativa.

Esta Política de Segurança Cibernética foi aprovada em reunião da diretoria da COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS FUNCIONÁRIOS DO GRUPO MAUÁ E EMPRESAS COLIGADAS LTDA. – COOPMAUÁ em 30/04/2019, atualizada em 07/04/2020, 30/07/2021, 14/06/2022, 30/01/2025 e revisada/atualizada em 14/09/2026.

A Política de Segurança Cibernética deverá ser divulgada para todos os membros estatutários, quadro social, colaboradores e prestadores de serviços.

São Gonçalo/RJ, 14 de setembro de 2026.

Ney Vieira Caldas – Diretor Responsável
Pela Política de Segurança Cibernética

Licelei Joaquim de Oliveira
Diretor Presidente

Fatima Cristina de Souza
Diretora Administrativa

Rafael de Almeida Ribeiro
Diretor Operacional