



COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS SERVIDORES DA COMLURB LTDA – COOPCOMLURB

POLÍTICA DE SEGURANÇA CIBERNÉTICA

PREÂMBULO

Este documento: Política de Segurança Cibernética tem como objetivo atender as determinações do Banco Central do Brasil, que através da Resolução BACEN 4.658/2018, revogada pela [Resolução CMN Nº 4.893, de 26 de fevereiro de 2021](#), 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 COOPCOMLURB, 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.

Este documento tem como finalidade não somente o atendimento à regulamentação vigente, mas também a promoção da cultura de segurança da informação e a mitigação proativa de riscos cibernéticos que possam comprometer as operações e a confiança dos associados da cooperativa.

Este documento está dividido 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.

1 – DO OBJETO E DO ÂMBITO DE APLICAÇÃO

A COOPCOMLURB 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 de Capital e Empréstimo” pela [Resolução CMN 5051](#) (art. 2º alínea III), 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 COOPCOMLURB não faz parte de nenhum Sistema Cooperativo de Crédito, sendo, portanto, considerada, uma Cooperativa “Solteira” 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 a 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 é um elemento fundamental para a manutenção da confiança dos associados, mitigação de riscos financeiros e legais, bem como para assegurar a continuidade dos negócios.

3 – PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Conforme está previsto na [Resolução CMN Nº 4.893/2021](#), devem ser previstos diversos aspectos da segurança cibernética e que irão nortear essa política:

I – Objetivos da Segurança Cibernética:

Assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

II – Procedimentos e controles para redução de vulnerabilidades:

Adoção de procedimentos e controles para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos objetivos da segurança cibernética. Tais procedimentos envolvem níveis adequados de acesso às informações, vigilância contínua e a contratação de sistemas confiáveis para processamento e armazenamento de dados.

III – Controles específicos:

Incluem a rastreabilidade da informação e o uso de equipamentos e programas confiáveis, como antivírus atualizados e manutenção preventiva constante. O armazenamento em nuvem deverá ser adotado como princípio de segurança confiável.

IV – Gestão integrada e contínua de riscos:

A gestão de riscos deve ser integrada e permanente, contemplando avaliação periódica e atualização dos controles para responder às novas ameaças e vulnerabilidades do ambiente tecnológico.

V – Registro e tratamento de incidentes:

O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, devem ser realizados com atenção constante. Deve-se monitorar tentativas de ataques cibernéticos e apurar incidentes, mesmo que não relevantes inicialmente, pois qualquer ocorrência pode indicar falhas nas defesas. Essas ocorrências devem ser debatidas nos diversos níveis operacionais da Cooperativa para aprimorar mecanismos preventivos.

VI – Diretrizes específicas para segurança cibernética:

a) Elaboração de cenários de incidentes para testes de continuidade de negócios, considerando situações que possam causar interrupções, acesso indevido a informações confidenciais, destruição de dados, bloqueio de acessos mediante resgate criminoso, entre outros.

b) Definição de procedimentos e controles para prevenção e tratamento de incidentes em empresas prestadoras de serviços terceirizados que manuseiem

dados sensíveis ou relevantes para as operações da Cooperativa. Essa relação deve ser estruturada com base na confiança técnica e jurídica, ancorada em contratos robustos e revisada periodicamente para garantir segurança jurídica e operacional.

c) Classificação dos dados e informações quanto à relevância, observando a proteção legal (Lei Complementar 105/2001) e a necessidade de sigilo e tratamento prioritário para informações sensíveis, com ciência dos colaboradores autorizados sobre as consequências de violações. Outros dados podem ter classificações mais flexíveis.

d) Definição dos parâmetros para avaliação da relevância dos incidentes, priorizando as informações protegidas por legislação vigente e, em seguida, outras classificações pertinentes conforme critérios internos.

VII – Política de revisão e disseminação:

A política deverá ser revisada periodicamente, com registro formal das versões e comunicação a todos os envolvidos, garantindo sua atualização conforme evolução tecnológica e regulatória.

Além disso, deverão ser implementados mecanismos para disseminação da cultura de segurança cibernética na Cooperativa, incluindo:

a) Programas de capacitação e avaliação periódica de membros estatutários e colaboradores, com inclusão específica de segurança cibernética.

b) Prestação de informações aos clientes e usuários sobre precauções no uso de produtos e serviços financeiros, reforçando a importância da segurança e do sigilo previsto na legislação.

c) Comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética, com participação ativa da diretoria e indicação de diretor responsável pela área.

VIII – Compartilhamento de informações sobre incidentes:

Iniciativas para compartilhamento de informações sobre incidentes relevantes mencionados no item V com outras cooperativas de crédito devem ser buscadas, visando a prevenção conjunta. Uma das formas é por meio das empresas de informática contratadas, que atendem diversas cooperativas e podem servir como elo para o compartilhamento, desde que autorizadas.

CONSIDERAÇÕES COMPLEMENTARES SOBRE OS INCISOS

Inciso I – Deverá ser contemplada a capacidade da cooperativa para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, situação essa 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 IV – 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 V – As diretrizes para registro e tratamento devem contemplar procedimentos com níveis compatíveis de complexidade e abrangência adequados à cooperativa.

4 – 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:

- 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.

4.1 – Regras do 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 CMN Nº 4.893/2021](#).
- 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.
- É recomendada a adoção de mecanismos de monitoramento contínuo dos recursos tecnológicos para identificação precoce de comportamentos suspeitos ou não autorizados.

4.2 Regras do Uso do Computador

- Os computadores disponibilizados para o usuário são de propriedade da cooperativa, e devem ser utilizados com zelo e os cuidados necessários para assegurar seu pleno funcionamento dentro da vida útil estimada de usos.
- 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 a 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.

4.3 - 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.

4.4 - Regras do Uso do Correio Eletrônico

- A cooperativa disponibiliza correio eletrônico para utilização dos usuários, no desempenho de suas funções profissionais, que pode ser o geral da cooperativa cooplurb@uol.com.br.
- Em caso de necessidade por qualquer que seja o motivo justificado e aprovado, poderá haver alteração no endereço geral, bem como, serem criados correios eletrônicos individuais.
- Em caso da necessidade de criar novos correios eletrônicos individuais, será de responsabilidade do colaborador designado a possuir todo o acesso ao conteúdo de mensagens, 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.

4.5 – Regras do Uso do Telefone

- A cooperativa disponibiliza telefone fixo para utilização dos membros estatutários e 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 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 as linhas 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 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, são passíveis de punições por força da [Lei Complementar 105/2001](#).

4.6 – 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.

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 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.

Previamente à contratação desses serviços, devem 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.

A Cooperativa tem contrato de Prestação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem com a Empresa R Barradas Fraga Informática Ltda, CNPJ 35.412.817/0001-05, com sede na Rua Maria Freitas, 42 – Sala 404 – Madureira/RJ, CEP 21.351-010, conforme contrato firmado arquivado na cooperativa.

Esta Política de Segurança Cibernética foi aprovada em Reunião da Diretoria da CECM dos Servidores da Comlurb Ltda. – COOPCOMLURB, em 06/05/2019, revisada em 18/03/2022, novamente revisada em 31/07/2023 e novamente revisada em 20/08/2025, devendo ser divulgada para todos os membros estatutários, usuários colaboradores, bem como, ao quadro social.

Rio de Janeiro, RJ, 20 de agosto de 2025.

Nelson Reis Quintella - Diretor Presidente:

Assinado por:
NELSON REIS QUINTELLA
1D68CBF66144455...

Candido Batista dos Santos - Diretor Financeiro:

Assinado por:
Candido Batista dos Santos
A8B17220194D4F7...

Hugo Rodrigues Goulart - Diretor Administrativo:

Assinado por:
HUGO RODRIGUES GOULART
1D68CBF66144455...