POLÍTICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

1. INTRODUÇÃO

A **Política de Segurança Cibernética** da **Cooperativa de Economia e Crédito Mútuo Aliança – Coopernitro** estabelece diretrizes, responsabilidades, procedimentos e controles destinados à proteção dos dados, das informações, dos ativos tecnológicos e dos sistemas utilizados pela Cooperativa, bem como define requisitos para a contratação, o monitoramento e a gestão de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem.

Esta política foi elaborada considerando o porte da Cooperativa, classificada no segmento S5, sua estrutura organizacional, perfil de risco, modelo de negócio, natureza das operações, complexidade dos produtos, serviços, atividades e processos, bem como a sensibilidade dos dados e das informações sob sua responsabilidade. Seu propósito é contribuir para a preservação da confidencialidade, integridade e disponibilidade das informações, reduzir a exposição a incidentes cibernéticos, fortalecer a resiliência operacional e assegurar a aderência à regulamentação aplicável do Conselho Monetário Nacional (CMN) e do Banco Central do Brasil (BCB).

2. OBJETIVO

Esta Política de Segurança Cibernética tem por objetivo estabelecer diretrizes, responsabilidades e controles para a gestão da segurança cibernética da **Cooperativa de Economia e Crédito Mútuo Aliança – Coopernitro**, de forma compatível com seu porte, perfil de risco, modelo de negócio e natureza das operações. Busca preservar a confidencialidade, a integridade e a disponibilidade dos dados, informações, ativos tecnológicos e sistemas da Cooperativa, bem como orientar a prevenção, detecção, resposta e recuperação diante de incidentes cibernéticos, incluindo a contratação e o monitoramento de serviços relevantes e de computação em nuvem, em conformidade com a regulamentação aplicável.

3. APLICABILIDADE

As diretrizes desta política aplicam-se a todos os componentes da estrutura organizacional, sendo Diretoria Executiva**,** Conselho Fiscal, colaboradores, terceiros, prestadores de serviços relevantes, fornecedores, associados e demais pessoas físicas ou jurídicas que tenham acesso a dados, informações, ambientes, ativos

tecnológicos, sistemas ou processos da Cooperativa, inclusive no contexto de serviços terceirizados, desenvolvimento de sistemas, integrações eletrônicas e computação em nuvem.

4. CONCEITOS

Para esta política definimos:

a. Segurança Cibernética: ações voltadas para preservar a disponibilidade, a integridade, a confidencialidade e a autenticidade, é um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação que é transmitida através das redes de comunicação, incluindo a internet e telefones celulares;

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

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

d. Incidente Cibernético: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança cibernética;

e. Risco Cibernético: ameaça à confidencialidade, integridade e disponibilidade das informações, exposição a danos e perdas resultantes da ocorrência de incidentes cibernéticos;

f. Ativos Cibernéticos: são os softwares, como um programa de computador, conectividades como acesso à internet, Banco Central do Brasil (BCB), Receita Federal do Brasil (RFB), as informações sigilosas de associados e componentes físicos, como servidores, estações de trabalho, notebooks etc.;

g. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou organização e que podem ser evitados por uma ação interna de segurança da informação.

5. RESPONSABILIDADES

De acordo com o porte, a estrutura, o perfil de risco e o modelo de negócio da Cooperativa ficam definidas as responsabilidades descritas nos itens a seguir.

5.1. DIRETORIA EXECUTIVA

São responsabilidades da Diretoria Executiva:

a. aprovar esta Política de Segurança Cibernética, bem como suas revisões, e assegurar sua compatibilidade com o porte, o perfil de risco, o modelo de negócio, a natureza das operações e a sensibilidade dos dados e das informações sob responsabilidade da Cooperativa
b. aprovar o Plano de Ação, o Plano de Respostas a Incidentes Relevantes e o Relatório Anual de Segurança Cibernética sobre a efetividade das ações adotadas;
c. assegurar a definição formal de papéis e responsabilidades, inclusive do diretor responsável e da área ou função responsável pelo processo de segurança cibernética;
d. promover supervisão tempestiva sobre riscos cibernéticos, incidentes relevantes, deficiências de controles, planos de correção, testes e contratações de serviços relevantes;
e. prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética;
f. manter comprometimento e apoio à aderência a Política de Segurança Cibernética de acordo com os objetivos e estratégias de negócios estabelecidas na Cooperativa;
g. fornecer claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário ao prestador de serviço responsável pelo processo de segurança cibernética;
h. prover recursos financeiros, humanos e tecnológicos compatíveis com a implementação, manutenção, monitoramento contínuo e aprimoramento da segurança cibernética e da continuidade de negócios.

5.2. DIRETOR RESPONSÁVEL PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA

São responsabilidades do diretor responsável pela Política de Segurança Cibernética:

a. propor atualizações desta Política de Segurança Cibernética, do Plano de Ação e do Plano de Resposta a Incidentes Relevantes, com base em mudanças regulatórias, avaliações de risco, incidentes ocorridos, testes, auditorias e lições aprendidas;
b. acompanhar a implementação e a efetividade das diretrizes, dos procedimentos e dos controles de segurança cibernética, inclusive quanto a terceiros relevantes;
c. assegurar a execução e o acionamento, quando cabível, do Plano de Ação e do Plano de Resposta a Incidentes Relevantes, incluindo escalonamento para a alta administração e comunicação regulatória quando aplicável;
d. assegurar o registro, o tratamento, o reporte e o acompanhamento dos incidentes relevantes e das deficiências identificadas, até sua adequada remediação;
e. elaborar o Relatório Anual de Segurança Cibernética sobre a implementação do Plano de Ação e do Plano de Resposta a Incidentes Relevantes com apoio do prestador de serviço responsável pelo processo de segurança cibernética e apresentá-lo para aprovação da Diretoria Executiva;
f. comunicar ao Banco Central do Brasil sobre a ocorrências de incidentes relevantes e das interrupções dos serviços que configurem uma situação de crise na Cooperativa;
g. informar ao Banco Central do Brasil sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem;
h. comunicar ao Banco Central do Brasil as providências tomadas para reinício das atividades após a interrupções dos serviços na Cooperativa.

O Diretor responsável pela Política de Segurança Cibernética poderá desempenhar outras funções na Cooperativa desde que não haja conflitos de interesses.

5.3. COORDENAÇÃO

São responsabilidades da Coordenação:

a. garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança de cibernética;
b. avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
c. designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
d. autorizar acessos aos colaboradores apenas quando forem realmente necessários.

5.4. PRESTADOR DE SERVIÇO RESPONSÁVEL PELA SEGURANÇA CIBERNÉTICA

São responsabilidades do prestador de serviço responsável pelo processo de segurança cibernética.

a. desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança Cibernética;
b. conduzir o processo de gestão de riscos de segurança cibernética;
c. conduzir a gestão de incidentes de segurança cibernética, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
d. conduzir a definição de controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas;
e. propor projetos e iniciativas para melhoria do nível de segurança cibernética da Cooperativa;
f. realizar o registro e o controle dos efeitos de incidentes relevantes;
g. realizar periodicamente testes e varreduras para detecção de vulnerabilidades;
h. executar e manter cópias de segurança dos dados e das informações;
i. comunicar ao Banco Central do Brasil (BCB) sobre a ocorrências de incidentes relevantes e das interrupções dos serviços que configurem uma situação de crise na Cooperativa;

j. informar ao BCB sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem;
k. comunicar ao BCB as providências tomadas para reinício das atividades após a interrupção dos serviços na Cooperativa.

5.5. DEMAIS INTEGRANTES COM ACESSO AOS DADOS OU SISTEMAS UTILIZADOS PELA COOPERATIVA

São responsabilidades dos demais integrantes com acesso aos dados ou sistemas utilizados pela Cooperativa:

a. notificar o prestador de serviço responsável pelo processo de segurança cibernética os incidentes de segurança que venha a tomar conhecimento e as violações desta Política de Segurança Cibernética;
b. utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de segurança cibernética;
c. responsabilizar pela segurança das informações e cumprir as determinações desta política, normas e padrões de segurança cibernética estabelecidos na Cooperativa.

6. RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, colaboradores, competidores etc.) como por exemplo:

a. ganhos financeiros através de roubo, manipulação ou adulteração de informações;
b. obter vantagens competitivas e informações confidenciais de clientes ou instituições concorrentes;

c. fraudar, sabotar ou expor a instituição invadida por motivos de vingança, ideias, políticas ou sociais;
d. praticar o terror e disseminar pânico e caos;
e. enfrentar desafios e/ou ter adoração por hackers famosos.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização.
As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.
Tanto instituições grandes como menores podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados sendo também essa necessidade um dos motivos da implementação desta Política.
Entre esses ativos cibernéticos estão:

a. Softwares, como um programa de computador;
b. Conectividades como acesso à internet, Banco Central, Receita Federal etc.;
c. Informações sigilosas de associados;
d. Componentes físicos, como servidores, estações de trabalho, notebooks etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central do Brasil, por meio da Resolução CMN nº 4.893/2021, alterada pela Resolução CMN nº 5.274/2025, têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

7. PRINCÍPIOS E PROCEDIMENTOS DA SEGURANÇA CIBERNÉTICA

Na implementação desta política considera o porte, perfil de risco, modelos dos negócios, bem como a natureza das operações e a complexidade dos produtos, serviços, atividades e processos atualmente praticados pela Cooperativa. Considera-

se, ainda, a sensibilidade dos dados e informações que estão sob suas responsabilidades.

Para atender esta política são baseados os seguintes princípios:

a. confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
b. integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);
c. disponibilidade: garantir que as informações estejam disponíveis às pessoas autorizadas.

Os ambientes, sistemas, computadores e redes da Coopernitro poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. Caberá a todos os colaboradores conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

Conforme a Resolução CMN nº 4.893/2021, alterada pela Resolução CMN nº 5.274/2025, os serviços de computação em nuvem abrangem a disponibilidade à Coopernitro, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

a. processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Coopernitro implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos;
b. implantação ou execução de aplicativos desenvolvidos ou adquiridos pela Coopernitro utilizando recursos computacionais de seus prestadores de serviços;
c. execução por meio de Internet dos aplicativos implantados ou desenvolvidos por prestadores de serviços da Coopernitro, com utilização de recursos computacionais do próprio prestador de serviços contratado.

A Coopernitro é responsável pela gestão dos serviços contratados incluindo as seguintes atividades:

a. análises de informações e de recursos adequados ao monitoramento dos serviços;
b. confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a prestadores de serviços;
c. cumprimento da legislação e da regulamentação vigente.

7.1. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações serão classificadas considerando a relevância, sensibilidade, criticidade e grau de sigilo para os negócios e para os associados nos seguintes níveis:

a. pública: são informações que possuem caráter informativo geral e que são direcionadas ao público em geral;
b. interna: são informações destinadas ao uso interno da Coopernitro e que estão disponíveis para todos os colaboradores;
c. restrita: são informações disponíveis apenas aos colaboradores específicos da Coopernitro, que as necessitem para exercer suas atribuições;
d. confidencial: são informações sigilosas de caráter estratégico para a Coopernitro e que estão disponíveis somente para a Diretoria Executiva e pessoas por ela autorizadas.

7.2. PROCEDIMENTOS DE CONTROLES DOS COLABORADORES

Os ambientes, sistemas, computadores e redes da Coopernitro poderão ser monitorados e gravados, com prévia notificação da informação, conforme previsto nas leis brasileiras.

Todos os colaboradores devem conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

As informações são classificadas de acordo com a confidencialidade e as proteções necessárias e, devem ser tratadas de forma sigilosa, de acordo com a regulamentação e a legislação vigentes, observada a finalidade do tratamento.

O acesso às informações só deve ser feito se devidamente autorizado, e o acesso deverá ser realizado por meio de credencial única, pessoal, intransferível e identificável, conforme as diretrizes de segurança da informação aprovada pela Coopernitro.

Quaisquer riscos às informações relacionados ao ambiente cibernético da Coopernitro devem ser comunicados por e-mail diretamente ao prestador de serviço responsável pelo processo de segurança cibernética com cópia para a Diretoria Executiva.

7.3. CENÁRIOS DE INCIDENTES

O prestador de serviço responsável pelo processo de segurança cibernética elabora cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela Coopernitro**,** que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios, levando-se em consideração para a elaboração desses cenários a ausência de ativos humanos ou tecnológicos, os testes são realizados para avaliação da continuidade de negócios.

7.4. AVALIAÇÃO DA RELEVÂNCIA DOS INCIDENTES DE SEGURANÇA

Os critérios a serem utilizados na avaliação da relevância dos incidentes na Coopernitro deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em dano ou possam ter a capacidade de causar interrupção nos processos de negócios, bem como perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

7.4.1. CLASSIFICAÇÃO DE RELEVÂNCIA DE INCIDENTES DE SEGURANÇA

A Cooperativa adota critérios objetivos para classificar a relevância de incidentes de segurança cibernética, garantindo que os esforços e recursos de resposta sejam priorizados de acordo com a criticidade de cada evento. A avaliação fundamenta-se na análise da frequência e do impacto potencial de cada ocorrência.

Um incidente será classificado como relevante quando apresentar potencial para causar prejuízos significativos, tais como:

a. **interrupção das operações**: impedimento do funcionamento de sistemas críticos ou interrupção na prestação de serviços essenciais aos associados;
b. **comprometimento da integridade dos dados**: perda, alteração indevida ou destruição de informações da Cooperativa ou de seus associados;
c. **ameaça à confidencialidade:** exposição de dados sigilosos ou sensíveis a pessoas não autorizadas, com violação da privacidade.
d. **dano à confiança e reputação**: risco à credibilidade da Cooperativa perante o mercado ou comprometimento da segurança das transações financeiras.

7.4.1. PROCEDIMENTOS DE REPORTE

Diante da detecção de qualquer comportamento anômalo nos sistemas ou falha de segurança, o colaborador deve comunicar imediatamente a Diretoria Executiva, prestador de serviços responsável pelo processo de segurança cibernética. Caberá a este prestador de serviços realizar a análise técnica necessária para determinar a relevância do incidente e conduzir as medidas de resposta e contingência cabíveis.

7.5. PROCEDIMENTOS DE CONTROLES

Como forma de reduzir as vulnerabilidades dos ativos de informação, a Cooperativa adota procedimentos e controles compatíveis com seu porte, perfil de risco, modelo de negócio e sensibilidade dos dados, observando, no mínimo, os requisitos regulatórios aplicáveis e a necessidade de comprovação por evidências auditáveis, considerando:

a. autenticação;
b. mecanismos de criptografia;
c. mecanismos de prevenção e detecção de intrusão;
d. mecanismos de prevenção de vazamento de informações;
e. mecanismos de proteção contra softwares maliciosos;
f. mecanismos de proteção da rede;
g. mecanismos da rastreabilidade para informações sensíveis e eventos relevantes;
h. gestão de cópias de segurança dos dados e das informações;

i. avaliação e correção de vulnerabilidades dos recursos computacionais e dos sistemas de informação;
j. controles de acessos e segmentação de rede de computadores;
k. definição e implementação de perfis de configuração segura de ativos de tecnologia;
l. gestão de certificados digitais;
m. requisitos de segurança para integração de sistemas de informação por meio de interfaces eletrônicas;
n. a realização periódica de testes e varreduras para detecção de vulnerabilidades;
o. ações de inteligência no ambiente cibernético, incluindo o monitoramento de informações de interesse da Cooperativa na internet, na *Deep Web*, na *Dark Web* e em grupos privados de comunicação, quando aplicável.

Os procedimentos e controles acima devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros, na aquisição de sistemas, no uso de sistemas desenvolvidos ou operados por terceiros com recursos computacionais da Cooperativa, no relacionamento com prestadores de serviços e na adoção de novas tecnologias empregadas em suas atividades, observada a necessidade de verificação, documentação, monitoramento e remediação das deficiências identificadas.

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

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

Na contratação de serviços relevantes de processamento e armazenamento de dados, de computação em nuvem e de outros serviços tecnológicos relevantes para a continuidade, a segurança ou a rastreabilidade das operações, no país ou no exterior, devem ser observados, no mínimo, requisitos de *due diligence*, avaliação de risco, cláusulas contratuais regulatórias, monitoramento contínuo, direito de acesso a

informações e auditoria, gestão de subcontratação, continuidade dos serviços e plano de saída, observados os seguintes aspectos:

a. ter a Política de Segurança Cibernética e Plano de Continuidade de Negócios;
b. manter registro e autorização em caso de mudanças ou alterações de serviços ou sistemas; e
c. ter relatórios de controles e gestão de incidentes.

A Coopernitro faz a verificação da capacidade potencial do prestador de serviços de forma a assegurar os seguintes requisitos:

a. cumprimento da legislação e da regulamentação em vigor;
b. permissão de acessos da Coopernitro aos dados e as informações a serem processadas ou armazenadas pelo prestador de serviços;
c. o prestador de serviços deve manter a confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas e armazenadas;
d. aderência a certificações que a Coopernitro possa exigir para a prestação do serviço a ser contratado;
e. identificação e segregação dos dados dos clientes Coopernitro por meio de controles físicos ou lógicos;
f. qualidade dos controles de acesso voltados à proteção dos dados e das informações dos associados da Coopernitro;
g. a Coopernitro deverá ter acesso aos relatórios de auditoria contratada pelo prestador de serviço e fornecimento de informações e de recursos de gestão adequados aos monitoramentos dos serviços as serem prestados;
h. os prestadores de serviços relevantes serão avaliados considerando a criticidade do tipo de serviços a ser prestado, bem como a sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas;
i. devem ser verificadas a adoção de controles que reduzam eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados pela internet.

7.6.1. CONTRATOS COM PRESTADORES DE SERVIÇOS RELEVANTES

A Cooperativa deve assegurar, em contrato ou instrumento equivalente, o direito de realizar auditorias, avaliações, testes e solicitações de evidências relacionadas à segurança cibernética e à continuidade de negócios dos prestadores de serviços relevantes, admitida a utilização de relatórios de auditoria independente ou especializada, desde que suficientes para fins de monitoramento e supervisão.

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

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

Em caso de extinção do contrato o prestador de serviço deverá transferir os dados ao novo prestador de serviços ou a própria Cooperativa e excluir os dados após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos. A empresa contratada deverá notificar a Cooperativa sobre a subcontratação de serviços relevantes para a Cooperativa.

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

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

Os contratos devem prever ainda permissão de acesso ao Banco Central do Brasil (BCB) nas seguintes informações:

a. contratos e aos acordos firmados para a prestação de serviços;
b. documentação e às informações referentes aos serviços prestados;
c. dados armazenados e às informações sobre seus processamentos;

d. cópias de segurança dos dados e das informações;
e. códigos de acesso aos dados e às informações;
f. adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil;
g. obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

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

a. a obrigação da empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados na alínea “g” do caput, que estejam em poder da empresa contratada;
b. a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observado que:
   - ✓ a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
   - ✓ a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

Os contratos devem prever, obrigatoriamente, a existência de planos de contingência testados pelo prestador de serviço para garantir a continuidade das operações em caso de interrupção.

7.6.2. COMUNICAÇÃO AO BANCO CENTRAL DO BRASIL

A Cooperativa deverá realizar as comunicações ao Banco Central do Brasil (BCB) relacionadas à contratação de serviços relevantes, incidentes relevantes e interrupções de serviços relevantes que configurem situação de crise, nos prazos, critérios, forma e procedimentos estabelecidos na regulamentação aplicável e em normas operacionais específicas.

A comunicação deverá conter, conforme o caso e a exigência regulatória aplicável, informações suficientes para identificação do serviço contratado, do prestador, da localização da prestação e do armazenamento, dos riscos envolvidos, dos controles adotados e dos fatos relevantes associados ao evento comunicado, incluindo:

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

As alterações contratuais que impliquem modificações nas informações contratuais devem ser comunicadas ao BCB no mínimo 10 (dez) dias após a alteração contratual.

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

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

No caso de inexistência de convênio citado nos itens anterior, a Coopernitro deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas. A Coopernitro deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações.

8. PROTEÇÃO E PREVENÇÃO AO RISCO CIBERNÉTICO

8.1. MITIGAÇÃO DOS RISCOS

A mitigação dos riscos cibernéticos constitui a base do conjunto de controles adotados pela Coopernitro para reduzir vulnerabilidades e limitar a probabilidade ou o impacto de eventos adversos. Esta seção reúne os controles estruturais e técnicos aplicáveis ao ambiente tecnológico, servindo de fundamento para as ações preventivas da seção 8.2, para o tratamento de incidentes da seção 8.3 e para as atividades de monitoramento e testes da seção 8.4.

Para esse fim, a Cooperativa mantém controles voltados à proteção dos ativos, à gestão de vulnerabilidades, à segurança de acessos e à resiliência do ambiente, observando, no mínimo, as seguintes práticas:

a. **gestão de ativos**: manutenção de inventário atualizado de hardware e software, permitindo o controle rigoroso sobre os ativos conectados à rede da Cooperativa;
b. **controle de acessos e software**: monitoramento periódico do ambiente tecnológico para identificação de dispositivos não autorizados e verificação da conformidade de licenciamento de softwares, coibindo a utilização de recursos não homologados;
c. **gestão de vulnerabilidades e atualizações**: manutenção dos sistemas operacionais e softwares em níveis atualizados (*patch management*), visando à mitigação de brechas de segurança conhecidas;
d. **testes de intrusão e conscientização**: realização periódica de testes de invasão (*pentests*) e simulações de *phishing*, com o objetivo de avaliar a robustez das defesas perimetrais e o nível de prontidão dos colaboradores diante de tentativas de engenharia social;

e. **<u>análise de riscos tecnológicos</u>**: execução sistemática de análises de vulnerabilidade na infraestrutura tecnológica, sendo o procedimento obrigatório sempre que houver alterações significativas no ambiente, atualizações de grande porte ou mudanças na arquitetura de rede;
f. **<u>simulação de incidentes e resiliência:</u>** realização periódica de testes e simulações do Plano de Respostas a Incidentes Relevantes, contemplando cenários de crise, a fim de validar a eficácia dos procedimentos de recuperação e a continuidade das operações.

Além dos controles técnicos e de monitoramento, a Coopernitro adota medidas administrativas e comportamentais destinadas à redução da exposição a riscos cibernéticos, incluindo o uso adequado dos recursos tecnológicos, a proteção de credenciais, a gestão de acessos e a pronta comunicação de impropriedades ou vulnerabilidades identificadas.

A Coopernitro disponibiliza aos colaboradores recursos tecnológicos necessários ao exercício de suas atividades, cabendo a cada usuário zelar pela integridade dos equipamentos, sistemas, acessos e informações sob sua responsabilidade. Esses recursos devem ser utilizados exclusivamente para finalidades profissionais e em conformidade com as normas internas da Cooperativa.

A instalação, cópia ou utilização de arquivos, programas, aplicativos ou quaisquer softwares em equipamentos da Coopernitro depende de autorização prévia do Diretor responsável pela Política de Segurança Cibernética, devendo ser observadas as regras de licenciamento, propriedade intelectual e segurança da informação aplicáveis.

As mensagens enviadas ou recebidas por meio do correio eletrônico corporativo, seus anexos e a navegação na internet realizada por meio dos recursos da Coopernitro poderão ser monitorados, observada a legislação aplicável e as normas internas da Cooperativa.

As credenciais de acesso, incluindo senhas, códigos e demais mecanismos de autenticação, são pessoais, intransferíveis e de responsabilidade exclusiva do usuário. As senhas não devem ser compartilhadas, anotadas em locais inseguros, armazenadas em arquivos desprotegidos ou baseadas em informações pessoais ou combinações óbvias. O usuário poderá ser responsabilizado pelo uso indevido de

suas credenciais, inclusive quando decorrente de compartilhamento, negligência ou descumprimento das normas internas.

Os usuários devem alterar suas senhas sempre que houver suspeita de comprometimento, vazamento, uso indevido ou acesso não autorizado, comunicando imediatamente o fato ao prestador de serviço responsável pelo processo de segurança cibernética e à Diretoria Executiva, quando aplicável.

A Diretoria Executiva acompanhará a efetividade dos controles adotados para mitigação dos riscos cibernéticos e promoverá, sempre que necessário, ações de correção, aprimoramento e reforço dos procedimentos internos, com o objetivo de prevenir incidentes, reduzir impactos e assegurar a melhoria contínua da segurança cibernética.

8.2. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Enquanto a seção 8.1 define os controles destinados à mitigação dos riscos, esta seção estabelece as ações preventivas e protetivas que orientam a conduta diária de colaboradores, terceiros e prestadores de serviços. O objetivo é assegurar que os controles sejam aplicados de forma contínua, tempestiva e aderente às rotinas operacionais da Coopernitro, especialmente no uso de recursos tecnológicos, credenciais, canais eletrônicos e informações sob responsabilidade da Cooperativa.

a. orientar colaboradores, terceiros e prestadores de serviços quanto ao uso seguro dos recursos tecnológicos, canais eletrônicos, credenciais de acesso e informações sob responsabilidade da Cooperativa;
b. reforçar práticas de autenticação segura, sigilo de senhas, concessão de acessos conforme necessidade de uso e revisão periódica de permissões;
c. manter procedimentos de proteção contra engenharia social, mensagens suspeitas, anexos maliciosos, links não confiáveis e tentativas de fraude eletrônica;
d. assegurar que cópias de segurança, registros de acesso, evidências de monitoramento e demais informações relevantes estejam disponíveis para verificação, auditoria e resposta a incidentes;
e. exigir que novas soluções, alterações relevantes em sistemas, integrações eletrônicas e serviços tecnológicos sejam avaliados previamente quanto aos riscos de segurança cibernética e continuidade operacional;

f. acompanhar a execução de ações corretivas decorrentes de vulnerabilidades, falhas de controle, incidentes, testes, auditorias ou recomendações técnicas;
g. promover registro, acompanhamento e reporte das ações preventivas e protetivas à Diretoria Executiva, sempre que necessário, para avaliação de efetividade e melhoria contínua.

8.3. TRATAMENTO DE INCIDENTES

Caso as medidas de mitigação, prevenção e proteção não sejam suficientes para evitar a ocorrência de um evento adverso, aplica-se o processo de tratamento de incidentes. Para os fins desta política, incidentes são eventos não planejados que afetem, ou possam afetar, a confidencialidade, a integridade, a disponibilidade, a continuidade ou a segurança dos dados, sistemas e serviços da Coopernitro, incluindo, entre outras, as seguintes situações:

a. queda de energia elétrica;
b. falha de um elemento de conexão ou servidor fora do ar;
c. ausência de conexão com internet;
d. sabotagem / terrorismo;
e. ataques DDOS sigla em inglês para *Distributed Denial of Service* (Negação de Serviço Distribuída);
f. indisponibilidade de acesso a Cooperativa.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato para que ele seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

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

Avaliar o incidente em conjunto com o Diretor Responsável pela Segurança Cibernética para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas. Analisar motivos e consequências imediatas, bem como a gravidade da situação.

Após a identificação e avaliação de um incidente, a Cooperativa adotará as seguintes medidas, de forma proporcional à gravidade e ao impacto identificado:

a. **avaliação de impacto**: realização de análise técnica para mensurar a extensão do incidente, considerando a criticidade dos processos afetados e o nível de comprometimento dos ativos de informação;
b. **medidas de contingência e continuidade**: ativação imediata de mecanismos de contingência, como o redirecionamento de canais de atendimento, redundância de links de dados ou outras soluções técnicas pré-estabelecidas no Plano de Continuidade de Negócios (PCN), para assegurar a manutenção dos serviços essenciais;
c. **análise de natureza delituosa**: em casos que envolvam suspeitas de sabotagem, atos ilícitos ou ameaças externas, a Cooperativa avaliará a necessidade de registro de boletim de ocorrência perante as autoridades competentes, sem prejuízo da adoção de outras medidas jurídicas ou forenses necessárias para a preservação de direitos.
d. **comunicação aos Órgãos Reguladores**: notificação tempestiva ao Banco Central do Brasil (BCB) sobre a ocorrência de incidentes relevantes ou interrupções de serviços que configurem situação de crise, observando-rigorosamente os critérios de relevância, os canais de comunicação oficiais e os prazos estabelecidos pela regulamentação vigente.

8.3.1. PROCEDIMENTOS PÓS-INCIDENTE E RECUPERAÇÃO

Após a contenção do incidente e a comunicação às equipes de resposta, as áreas responsáveis pela segurança cibernética devem realizar uma avaliação detalhada para verificar a integridade dos dados e o status operacional dos sistemas afetados, considerando:

Após o incidente ter sido resolvido com a contingência da segurança cibernética e demais equipes chaves notificados, as áreas devem verificar se os dados estão faltando ou foram corrompidos ou outros problemas. Caso seja identificado que a Coopernitro perdeu informações ou dados**,** a Diretoria Executiva e equipe de contingência deverão ser informados imediatamente.

a. **verificação de integridade:** as áreas responsáveis devem realizar auditoria minuciosa para identificar eventuais perdas, corrupções ou indisponibilidades de dados, assegurando que o ambiente esteja íntegro para a retomada das operações;

b. **reporte de perda de informações:** caso seja confirmada a perda ou comprometimento de dados, a Diretoria Executiva e a equipe de contingência devem ser formalmente cientificadas de imediato, em conformidade com os protocolos de gestão de riscos da Cooperativa;
c. **plano de retomada e melhoria contínua:** para o restabelecimento da normalidade, a equipe técnica e de gestão deve definir e executar um plano de recuperação, contemplando:
    i. a reconstrução de sistemas e a restauração de backups, conforme as estratégias de continuidade de negócios;
    ii. a análise crítica das causas do incidente (*root cause analysis*);
    iii. a implementação de novas medidas preventivas e ajustes de segurança, visando mitigar a recorrência de eventos similares e fortalecer a resiliência cibernética da Cooperativa.

8.4. MONITORAMENTO E TESTES

O monitoramento e os testes têm a finalidade de verificar a efetividade dos controles previstos nas seções anteriores, identificar anomalias em tempo hábil, apoiar a detecção de vulnerabilidades e subsidiar a melhoria contínua da segurança cibernética. Essas atividades complementam a mitigação, a prevenção e o tratamento de incidentes, fornecendo evidências para avaliação da Diretoria Executiva e para eventuais ajustes nos procedimentos internos.

O ambiente de TI da Coopernitro deve ser supervisionado e monitorado de forma compatível com seu porte, perfil de risco e criticidade dos processos, com atenção especial a eventos que possam indicar tentativa de ataque, uso indevido de recursos, indisponibilidade, falha de controle ou exposição indevida de informações.

a. invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de *hackers*;
b. comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas;
c. comprometimento de estações de trabalho decorrente de cliques em link malicioso (“*phishing*”);

d. exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com condições internamente estabelecidas;
e. vazamento de informações durante tráfego de dados não criptografados.

Os testes de cibersegurança devem ser realizados periodicamente ou sempre que houver alterações relevantes no ambiente tecnológico, com o objetivo de validar a efetividade dos controles, identificar vulnerabilidades e apoiar a priorização de correções. A verificação deve considerar, entre outros aspectos:

a. uso da capacidade instalada da rede e dos equipamentos;
b. tempo de resposta no acesso à internet e aos sistemas críticos da Coopernitro;
c. períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Coopernitro;
d. vulnerabilidades que possam causar incidentes (vírus, trojans, furtos, acessos indevidos etc.).

A Coopernitro também tem como ferramenta de controle um Checklist de Conformidade de Ambiente de TI, com periodicidade trimestral, elaborado a partir de suas políticas internas e das normas vigentes do órgão fiscalizador.
Esta ferramenta auxilia à Diretoria Executiva e os colaboradores, a organizar os trabalhos, de forma a alcançar os resultados desejados de acordo com as metas preestabelecidas, realizando o monitoramento periódico da conformidade de processos e atividades com as normas internas.

9. CENÁRIOS DE INCIDENTES E AVALIAÇÃO DE FORNECEDORES

Anualmente, a Coopernitro realizará a avaliação das empresas que prestam serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados, visando observar se naquele período foram constatadas ocorrências que afetaram o atendimento aos associados.
Caso tenham ocorridos quaisquer fatos, deve-se contatar os fornecedores para obterem justificativa para tais ocorrências. Essas justificativas serão analisadas pela Diretoria Executiva que definirá manter o contrato com os fornecedores, pesquisar com outras Cooperativas clientes desse mesmo fornecedor, eventuais críticas quanto

ao serviço prestado. Avaliar novas opções no mercado, sempre destacando a referência de atender outras Cooperativas, se for o caso. Dependendo da situação ocorrida, a Diretoria Executiva analisará sua relevância e procederá à comunicação ao Banco Central do Brasil.

9.1. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES COM OUTRAS INSTITUIÇÕES

O compartilhamento de informações sobre incidentes cibernéticos relevantes poderá ser realizado por intermédio da Federação Nacional das Cooperativas de Crédito (FNCC), por meio do registro na Central de Atendimento.

9.2. REFORÇO NA RESILIÊNCIA OPERACIONAL

A Cooperativa pauta sua Política de Segurança Cibernética na promoção da resiliência operacional, visando garantir a continuidade, integridade e disponibilidade dos serviços, mesmo em cenários de incidentes severos.

A Cooperativa realizará, periodicamente, testes de estresse cibernético e simulações de incidentes que considerem a interrupção de serviços críticos.

Os processos de gestão de incidentes incluem critérios de classificação de "incidentes relevantes" baseados no impacto à reputação e à continuidade dos serviços aos associados.

10. PLANO DE AÇÃO, PLANO DE RESPOSTAS A INCIDENTES RELEVANTES E RELATÓRIO DE INCIDENTES RELEVANTES

Para fins desta Política, o Plano de Ação, o Plano de Respostas a Incidentes Relevantes e o Relatório de Incidentes Relevantes são instrumentos distintos e complementares.

O Plano de Ação orienta a implementação e o aprimoramento das medidas de segurança cibernética; o Plano de Respostas a Incidentes Relevantes estabelece os procedimentos de atuação diante de incidentes classificados como relevantes; e o Relatório de Incidentes Relevantes registra e consolida as informações sobre incidentes relevantes efetivamente ocorridos, as providências adotadas, os impactos identificados e as ações de correção e melhoria decorrentes.

O **Plano de Ação** contempla as medidas, responsáveis, prazos, evidências e controles necessários para adequar a estrutura organizacional e operacional da Cooperativa aos princípios e diretrizes desta Política, inclusive quanto à prevenção, mitigação, monitoramento, testes, correção de vulnerabilidades e melhoria contínua da segurança cibernética.

O Plano de Ação abordará os cenários de incidentes a serem avaliados nos testes de continuidade de negócios, considerando a avaliação de risco dos incidentes por níveis de impacto nos negócios, classificados como gravíssimo, grave, médio, baixo e muito baixo, como:

a. identificar os incidentes de segurança cibernética;
b. registrar os eventos que acarretaram problemas de segurança/continuidade;
c. direcionar medidas paliativas a incidentes ocorridos;
d. criar evidências e registros para medidas corretivas;
e. acionar o plano de continuidade dos negócios;
f. reportar os incidentes de segurança cibernética;
g. adotar iniciativas para compartilhamento de informações sobre incidentes relevantes com outras instituições.

O **Plano de Respostas a Incidentes Relevantes** define as rotinas, procedimentos, controles, tecnologias, responsáveis, canais de comunicação, critérios de escalonamento, medidas de contenção, recuperação, continuidade e reporte aplicáveis quando houver incidente relevante de segurança cibernética, observados os critérios de relevância e a regulamentação aplicável. O Plano de Respostas a Incidentes Relevantes será acionado quando os critérios de relevância forem atendidos.

O **Relatório de Incidentes Relevantes** deverá ser elaborado sempre que ocorrer incidente relevante, contendo, no mínimo, a descrição do evento, data e horário de identificação, sistemas, processos ou serviços afetados, avaliação de impacto, classificação de relevância, medidas de contenção e recuperação adotadas, responsáveis envolvidos, comunicações realizadas, situação de encerramento, lições aprendidas e ações corretivas ou preventivas definidas. O Relatório de Incidentes Relevantes será utilizado para formalizar o registro do incidente relevante ocorrido,

documentar seus efeitos e evidenciar as providências adotadas. Esses instrumentos deverão ser aprovados pelo Diretor responsável pela Política de Segurança Cibernética e revisados, no mínimo, anualmente ou sempre que houver alteração relevante no ambiente, nos riscos, nos controles ou na regulamentação aplicável.

11. RELATÓRIO ANUAL DE SEGURANÇA CIBERNÉTICA

O Relatório Anual de Segurança Cibernética deverá consolidar, de forma objetiva, verificável e baseada em evidências, a avaliação da implementação do Plano de Ação, do Plano de Respostas a Incidentes Relevantes e dos Relatórios de Incidentes Relevantes eventualmente elaborados no período, incluindo a efetividade dos procedimentos, controles e tecnologias adotados pela Coopernitro para prevenção, detecção, resposta, recuperação e melhoria contínua da segurança cibernética, em conformidade com a Resolução CMN nº 4.893/2021, alterada pela Resolução CMN nº 5.274/2025.

A Coopernitro emitirá anualmente, com data-base de 31 de dezembro, Relatório Anual de Segurança Cibernética referente à implementação do Plano de Ação e do Plano de Resposta a Incidentes Relevantes, observando seu porte, perfil de risco, modelo de negócio, natureza das operações, complexidade dos produtos, serviços, atividades e processos, bem como a sensibilidade dos dados e das informações sob sua responsabilidade.

O relatório deverá ser elaborado até 31 de março do ano subsequente à data-base, submetido ao Diretor responsável pela Política de Segurança Cibernética e apresentado à Diretoria Executiva para ciência, avaliação e aprovação, com registro em ata quando aplicável.

O Relatório Anual deverá contemplar, no mínimo, as seguintes informações:

a. avaliação da efetividade da implementação da Política de Segurança Cibernética, do Plano de Ação, do Plano de Respostas a Incidentes Relevantes e dos Relatórios de Incidentes Relevantes elaborados no período;
b. resumo dos resultados obtidos na implementação das rotinas, procedimentos, controles e tecnologias utilizados na prevenção, detecção, resposta e recuperação de incidentes;
c. relação dos incidentes relevantes relacionados ao ambiente cibernético ocorridos no período, incluindo descrição sintética, data de ocorrência, áreas

ou serviços afetados, impacto, medidas adotadas, situação de encerramento e eventuais comunicações realizadas ao Banco Central do Brasil, quando aplicável;

d. resultados dos testes de continuidade de negócios e das simulações de cenários de incidentes, especialmente aqueles que envolvam indisponibilidade de serviços críticos, perda de integridade, comprometimento de confidencialidade ou interrupção operacional;
e. resultados dos testes de intrusão, testes, varreduras e análises periódicas para detecção de vulnerabilidades, incluindo a identificação das vulnerabilidades relevantes, a classificação de criticidade, os responsáveis pelo tratamento, os prazos definidos e os planos de ação estabelecidos para correção;
f. avaliação dos procedimentos e controles mínimos previstos na regulamentação aplicável, incluindo autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, proteção contra softwares maliciosos, rastreabilidade, cópias de segurança, gestão de vulnerabilidades, controles de acesso, configuração segura de ativos, proteção de rede, certificados digitais, integração segura por interfaces eletrônicas e ações de inteligência cibernética;
g. avaliação dos serviços relevantes de processamento, armazenamento de dados, computação em nuvem e demais serviços tecnológicos críticos, quando existentes, incluindo eventos ocorridos no período, desempenho dos prestadores, evidências de monitoramento, conformidade contratual e necessidade de ações corretivas;
h. indicação das melhorias implementadas, das deficiências identificadas, das recomendações pendentes, dos planos de correção em andamento e do acompanhamento das ações até sua conclusão.

A avaliação constante do Relatório Anual deverá ser suportada por evidências documentais, tais como registros de incidentes, atas, relatórios de testes e varreduras, relatórios de fornecedores, registros de correção de vulnerabilidades, evidências de backup, controles de acesso, registros de monitoramento, comunicações internas e externas, planos de ação, pareceres técnicos e demais documentos que comprovem a implementação e a efetividade das medidas adotadas.

Sempre que aplicável, o relatório poderá apresentar indicadores quantitativos e qualitativos, incluindo quantidade de incidentes registrados, incidentes relevantes, vulnerabilidades identificadas e corrigidas, tempo médio de tratamento, testes realizados, treinamentos concluídos, pendências em aberto, ações corretivas executadas e nível de aderência aos controles previstos nesta Política.

As conclusões do Relatório Anual deverão indicar o nível de efetividade dos controles, os principais riscos residuais, as prioridades de tratamento para o período seguinte e as recomendações de aprimoramento da Política de Segurança Cibernética, do Plano de Ação e do Plano de Resposta a Incidentes Relevantes.

O Relatório Anual e as evidências que lhe dão suporte deverão permanecer arquivados e disponíveis ao Banco Central do Brasil pelo prazo mínimo previsto na regulamentação aplicável, observados os critérios de confidencialidade, integridade, rastreabilidade e disponibilidade das informações.

12. DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética deve ser divulgada aos colaboradores da Coopernitro e às empresas prestadoras de serviços relevantes, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

Para divulgação desta Política de Segurança Cibernética, a Coopernitro adotará as seguintes ações:

a. divulgação desta política à Diretoria Executiva, ao Conselho Fiscal, aos colaboradores, associados, terceiros e prestadores de serviços relevantes, ou àqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados, com evidência por meio de assinatura do Termo de Ciência;
b. divulgação no site aos associados e ao público, do resumo contendo as linhas gerais desta política.

13. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

A Coopernitro adotará os seguintes procedimentos para disseminação da cultura de segurança cibernética:

a. promover programas de capacitação e avaliação periódica de todos os colaboradores;
b. prestar informações aos usuários finais sobre os cuidados na utilização de produtos e serviços oferecidos;
c. manter o comprometimento da Diretoria Executiva com melhorias contínuas relacionados à segurança cibernética.

14. DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA

Devem ficar à disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos os seguintes documentos:

a. ata de Reunião da Diretoria Executiva com o registro referente a implantação e implementação a Política de Segurança Cibernética;
b. documento relativo ao Plano de Ação para implementação e aprimoramento da Política de Segurança Cibernética;
c. documento relativo ao Plano de Respostas a Incidentes Relevantes de Segurança Cibernética;
d. Relatórios de Incidentes Relevantes elaborados em razão de incidentes relevantes ocorridos, quando aplicável;
e. Relatório Anual de Segurança Cibernética sobre a implementação do Plano de Ação, do Plano de Respostas a Incidentes Relevantes e dos Relatórios de Incidentes Relevantes eventualmente elaborados no período;
f. documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem (se houver);
g. documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra (se houver);
h. contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem*; **(se houver);***
i. dados, registros e informações relativas aos mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da Política de Segurança Cibernética, do Plano de Ação e de Respostas a Incidentes Relevantes e dos requisitos para contratação de serviços de

processamento e armazenamento de dados e de computação em nuvem (se houver).

15. TREINAMENTO

A Cooperativa estabelece, anualmente, programa de conscientização e capacitação em segurança cibernética destinado a Diretoria Executiva, ao Conselho Fiscal e aos colaboradores, com o objetivo de assegurar o conhecimento, a observância e o cumprimento das diretrizes, dos procedimentos e dos controles previstos nesta Política, bem como de disseminar as responsabilidades específicas de cada público envolvido.

16. PERIODICIDADE DE REVISÃO

Esta Política será revisada anualmente, ou em decorrência de apontamentos de auditorias ou mudanças nas regulamentações, assegurando a sua contínua pertinência, adequação e eficácia.

17. POLÍTICA INTERNA DE PRIVACIDADE E DADOS

Todos os procedimentos e diretrizes desta política são realizados em conformidade com a Política Interna de Privacidade e Dados da Cooperativa de Economia e Crédito Mútuo Aliança, a qual dispõe sobre o tratamento de dados em observância a Lei nº 13.709/2018 - LGPD.

18. CONSIDERAÇÕES FINAIS

A Diretoria Executiva compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta política. Os indícios ou irregularidades devem ser comunicados ao prestador de serviço responsável pelo processo de segurança cibernética e ao diretor responsável pela segurança cibernética.

O cumprimento desta Política de Segurança Cibernética é de responsabilidade da Diretoria Executiva, do Conselho Fiscal, dos colaboradores, terceiros, prestadores de serviços relevantes e daqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados. A presente Política também poderá ser alterada sem prévio aviso em virtude de alterações legislativas.

Todas as observações e ocorrências, assim como ações a serem aprimoradas para atualização desta Política, serão inseridas em Ata da Diretoria Executiva.

Este normativo foi aprovado pela Diretoria Executiva e passa a vigorar na data de sua publicação.

19. REFERÊNCIAS NORMATIVAS

As referências normativas a seguir indicam as normas e diretrizes consideradas na elaboração desta política:

Normativo	Data	Órgão Regulador	Epígrafe
Resolução nº 4.658	26/04/2018	Conselho Monetário Nacional (CMN)	Dispõe 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 e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. ***Normativo revogado pela Resolução CMN nº 4.893/2021, devendo ser tratado apenas como referência histórica.***
Lei nº 13.709	14/08/2018	Planalto	Lei Geral de Proteção de Dados Pessoais (LGPD).
Resolução nº 4.893	26/02/2021	Conselho Monetário Nacional (CMN)	Dispõe 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 autorizadas a funcionar pelo Banco Central do Brasil.
Resolução nº 5.274	18/12/2025	Conselho Monetário Nacional (CMN)	Altera a Resolução CMN nº 4.893/2021 para reforçar e detalhar os controles mínimos obrigatórios de segurança cibernética, tornando-os mais objetivos, verificáveis e auditáveis, inclusive quanto a autenticação, criptografia, intrusão, prevenção de vazamento, rastreabilidade, backup, vulnerabilidades, acesso, hardening, proteção de rede, certificados digitais, interfaces eletrônicas e inteligência cibernética.

20. ANEXOS (MODELOS DE RELATÓRIOS)

O quadro a seguir apresenta a relação dos anexos que integram esta Política:

Anexos	**Modelos de Relatórios**
Anexo I	Plano de Ação de Segurança Cibernética
Anexo II	Plano de Respostas a Incidentes Relevantes de Segurança Cibernética
Anexo III	Relatório de Respostas a Incidentes Relevantes de Segurança Cibernética
Anexo IV	Relatório Anual de Segurança Cibernética
Anexo V	Resumo Política de Segurança Cibernética
Anexo VI	Termo de Ciência para Prestadores de Serviços

São Paulo, 30 de julho de 2026.

_____

Cláudio Nolasco
Presidente

_____

Eric Fernando Tomboly
Vice-Presidente

Política de Segurança Cibernética_versao07_30.07.2026.pdf

Documento número #3dfd5735-127d-4d17-89bb-f5b45a44c125

Hash do documento original (SHA256): 3f8ca3d97cd5366febd75d59181cc622ee593ad06cb60c160485824bff237721

Assinaturas

ERIC FERNANDO TOMBOLY
CPF: 277.209.688-24
Assinou em 31 jul 2026 às 14:37:40

CLAUDIO NOLASCO
CPF: 006.053.628-40
Assinou em 30 jul 2026 às 16:21:13

Log

30 jul 2026, 16:01:24	Operador com email renata.paschoalato@coopernitro.com.br na Conta 9becfaed-5ed3-4403-b150-af1283761c67 criou este documento número 3dfd5735-127d-4d17-89bb-f5b45a44c125. Data limite para assinatura do documento: 29 de agosto de 2026 (16:01). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
30 jul 2026, 16:01:48	Operador com email renata.paschoalato@coopernitro.com.br na Conta 9becfaed-5ed3-4403-b150-af1283761c67 adicionou à Lista de Assinatura: eric.tomboly@coopernitro.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo ERIC FERNANDO TOMBOLY.
30 jul 2026, 16:01:48	Operador com email renata.paschoalato@coopernitro.com.br na Conta 9becfaed-5ed3-4403-b150-af1283761c67 adicionou à Lista de Assinatura: claudionolasco@coopernitro.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo CLAUDIO NOLASCO e CPF 006.053.628-40.
30 jul 2026, 16:21:13	CLAUDIO NOLASCO assinou. Pontos de autenticação: Token via E-mail claudionolasco@coopernitro.com.br. CPF informado: 006.053.628-40. IP: 177.60.99.46. Localização compartilhada pelo dispositivo eletrônico: latitude -23.708 e longitude -46.5506. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1488.0 disponibilizado em https://app.clicksign.com.
31 jul 2026, 14:37:40	ERIC FERNANDO TOMBOLY assinou. Pontos de autenticação: Token via E-mail eric.tomboly@coopernitro.com.br. CPF informado: 277.209.688-24. IP: 152.244.64.151. Componente de assinatura versão 1.1488.0 disponibilizado em https://app.clicksign.com.

31 jul 2026, 14:37:48	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 3dfd5735-127d-4d17-89bb-f5b45a44c125.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001