POLÍTICA DE SEGURANÇA CIBERNÉTICA

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

SUMÁRIO

1 – INTRODUÇÃO 3
2 – OBJETIVO 3
3 – REGULAMENTAÇÃO 3
4 – APLICABILIDADE 3
5 – CONCEITOS 4
6 – RESPONSABILIDADES 4
7 – RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS 7
8 – PRINCÍPIOS, E PROCEDIMENTOS DA SEGURANÇA CIBERNÉTICA 8
8.1. CLASSIFICAÇÃO DAS INFORMAÇÕES 10
8.2. PROCEDIMENTOS DE CONTROLES DOS COLABORADORES 10
8.3. CENÁRIOS DE INCIDENTES 11
8.4. AVALIAÇÃO DA RELEVÂNCIA DOS INCIDENTES 11
8.5. PROCEDIMENTOS DE CONTROLES 11
8.6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM 12
9 – CENÁRIOS DE INCIDENTES E AVALIAÇÃO DE FORNECEDORES 16
9.1. MITIGAÇÃO DOS RISCOS 16
9.2. AÇÕES DE PREVENÇÃO E PROTEÇÃO 17
9.3. TRATAMENTO DE INCIDENTES 17
9.4. MONITORAMENTO E TESTES 19
10 – CENÁRIOS DE INCIDENTES E AVALIAÇÃO DE FORNECEDORES 20
11 – PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES RELEVANTES 21
12 – RELATÓRIO ANUAL DE SEGURANÇA CIBERNÉTICA 21
13 – DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA 22
14 – DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA 22
15 – DOCUMENTOS À DISPOSIÇÃO DO BANCO CENTRAL 22
16 – PERIOCIDADE DE REVISÃO 23
17 – POLÍTICA INTERNA DE PRIVACIDADE E DADOS 23
18 – CONSIDERAÇÕES FINAIS 23

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

1. INTRODUÇÃO

A **Política de Segurança Cibernética** dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pela **Cooperativa de Economia e Crédito Mútuo Aliança – Coopernitro**.

A elaboração desta política considerou o porte da Cooperativa, classificada como segmento S5, e em conjunto considerou também a complexidade; a estrutura; o perfil de risco; o modelo de negócio; a natureza das operações; a complexidade dos produtos, serviços, atividades e processos; a sensibilidade dos dados e das informações sob responsabilidade da instituição, buscando assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Cooperativa.

2. OBJETIVO

Esta Política de Segurança Cibernética tem como objetivo prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, e assegurar a proteção dos ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo dos negócios com o intuito de aplicar os princípios e diretrizes de proteção das informações consideradas sensíveis da Cooperativa e de seus associados.

3. REGULAMENTAÇÃO

A regulamentação associada a esta Política são: Resolução CMN nº 4.658/2018 revogada pela Resolução CMN nº 4.893/2021 Política de Segurança Cibernética e Lei 13.709/2018 Lei Geral de Proteção de Dados Pessoais – LGPD.

4. APLICABILIDADE

Esta política aplica-se a todos os componentes da estrutura organizacional, sendo Diretoria Executiva**,** Conselho Fiscal, colaboradores, terceiros, prestadores de serviços relevantes, associados e aqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

5. CONCEITOS

Para esta política definimos:

a. 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.;

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. 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;

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.

6. 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.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

6.1. DIRETORIA EXECUTIVA

São responsabilidades da Diretoria Executiva:

a. aprovar esta Política de Segurança Cibernética, o Plano de Ação e de Respostas a Incidentes Relevantes e o Relatório Anual de Segurança Cibernética sobre a implementação do plano de ação e de respostas a incidentes relevantes;
b. prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética;
c. manter comprometimento e apoio à aderência a Política de Segurança Cibernética de acordo com os objetivos e estratégias de negócios estabelecidas na Cooperativa;
d. fornecer claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário ao prestador de serviço responsável pelo processo de segurança cibernética;
e. fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança cibernética.

6.2. DIRETOR RESPONSÁVEL PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA

São responsabilidades do diretor responsável pela Política de Segurança Cibernética:

a. propor melhorias nas diretrizes da Política de Segurança Cibernética e no Plano de Ação e de Respostas a Incidentes Relevantes;
b. acompanhar se as diretrizes da política estão sendo executadas;
c. executar o Plano de Ação e de Respostas a Incidentes Relevantes;
d. elaborar o Relatório Anual de Segurança Cibernética sobre a implementação do Plano de Ação e de Respostas a Incidentes Relevantes com apoio do prestador de serviço responsável pelo processo de segurança cibernética e apresentá-lo para aprovação da Diretoria Executiva;
e. 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;
f. informar ao Banco Central do Brasil sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

g. 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 pode desempenhar outras funções na Cooperativa desde que não haja conflitos de interesses.

6.3. 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.

6.4. 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. realizar o registro e o controle dos efeitos de incidentes relevantes;
f. realizar periodicamente testes e varreduras para detecção de vulnerabilidades;
g. executar e manter cópias de segurança dos dados e das informações;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

h. propor projetos e iniciativas para melhoria do nível de segurança cibernética da Cooperativa.

6.5. 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.

7. 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:

- ganhos financeiros através de roubo, manipulação ou adulteração de informações;
- obter vantagens competitivas e informações confidenciais de clientes ou instituições concorrentes;
- fraudar, sabotar ou expor a instituição invadida por motivos de vingança, ideias, políticas ou sociais;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

- praticar o terror e disseminar pânico e caos;
- 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:

- ✓ Softwares, como um programa de computador;
- ✓ Conectividades como acesso à internet, Banco Central, Receita Federal etc.;
- ✓ Informações sigilosas de associados;
- ✓ 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 através das Resoluções CMN 4.658/2018 e 4.893/2021, 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.

8. PRINCÍPIOS E PROCEDIMENTOS DA SEGURANÇA CIBERNÉTICA

Na implementação desta política considerou-se o porte, perfil de risco, modelos dos negócios, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais da Cooperativa. Considerou-se também 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;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

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 4.658/2018 e 4.893/2021, os serviços de computação em nuvem abrangem a disponibilidade da 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.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

8.1. 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.

8.2. 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.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

8.3. 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.

8.4. AVALIAÇÃO DA RELEVÂNCIA DOS INCIDENTES

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.

8.5. PROCEDIMENTOS DE CONTROLES

Como forma de reduzir as vulnerabilidades dos ativos de informação, a Coopernitro adota procedimentos e os controles baseados em:

a. autenticação;
b. criptografia;
c. prevenção e detecção de intrusão;
d. prevenção de vazamento de informações;
e. a realização periódica de testes e varreduras para detecção de vulnerabilidades;
f. proteção contra softwares maliciosos;
g. mecanismos da rastreabilidade para informações sensíveis;
h. controles de acessos e segmentação de rede de computadores;
i. manutenção de cópias de segurança dos dados e das informações.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

8.6. 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 e de computação em nuvem, no país ou no exterior devem ser considerados os seguintes requisitos à empresa contratada:

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

A Coopernitro faz a verificação da capacidade do potencial 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;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

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.

8.6.1. CONTRATOS COM PRESTADORES DE SERVIÇOS

Os contratos firmados com as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever a indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados que poderão ser armazenados, processados e gerenciados, bem como adoção de medidas de segurança para transmissão de armazenamento de dados. Enquanto o contrato estiver vigente, deve prever a manutenção da segregação dos dados e dos controles de acessos para proteção das informações dos clientes.

Em caso de extinção do contrato o prestador de serviço deverá transferir os dados ao novo prestador de serviços ou a própria Cooperativa 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.

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 nas seguintes informações:

a. contratos e aos acordos firmados para a prestação de serviços;
b. documentação e às informações referentes aos serviços prestados;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

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.

8.6.2. COMUNICAÇÃO AO BANCO CENTRAL DO BRASIL

A Coopernitro deverá informar previamente ao Banco Central do Brasil a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem. Essa comunicação deve ser realizada com até 60 (sessenta) dias antes da contratação dos serviços e deve conter as seguintes informações:

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

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 Banco Central no mínimo 60 (sessenta) dias antes 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.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

9. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

9.1. MITIGAÇÃO DOS RISCOS

A Coopernitro estabeleceu um conjunto de medidas buscando mitigar os riscos de forma a impedir previamente a ocorrência de um ataque cibernético.

A Coopernitro oferece aos colaboradores uma completa estrutura tecnológica para o exercício de suas atividades, sendo responsabilidade de cada colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob seus cuidados, como computador, notebook, acesso à internet, e-mail, entre outros. Os equipamentos disponibilizados aos colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Cooperativa.

A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da Coopernitro depende de autorização prévia do Diretor responsável pela Política de Segurança Cibernética, devendo observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes.

As mensagens enviadas ou recebidas por meio de correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação na internet, mediante equipamentos da Coopernitro poderão ser monitoradas.

As senhas para acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (word, excel etc.); devem ser compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

De modo a atingir os resultados esperados dos controles adotados na prevenção aos ataques cibernéticos, a direção da Coopernitro está sempre atenta ao cumprimento das normas, e assim, evitar ou minimizar os riscos, caso aconteçam. Qualquer impropriedade identificada, a Diretoria Executiva é relatada e promovida a correção o mais rápido possível.

9.2. AÇÕES DE PREVENÇÃO E PROTEÇÃO

As ações de prevenção e proteção da Coopernitro a fim de manter funcionamento e efetividade da segurança cibernética seguem os seguintes requisitos:

a. manter relatório de inventários de hardware e software;
b. verificar com frequência se há na Cooperativa computadores/notebooks não autorizados ou software não licenciado;
c. manter os sistemas operacionais e software atualizados;
d. monitorar rotinas de backup, executando testes regulares de restauração dos dados;
e. realizar frequentemente testes de invasão externa e *phishing*;
a. fazer análises de vulnerabilidade na estrutura tecnológica da Cooperativa frequentemente ou em situações que houver mudança significativas;
b. fazer teste do plano de ação e de respostas a incidentes com simulação de cenários.

9.3. TRATAMENTO DE INCIDENTES

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Cooperativa, como por exemplo:

a. queda de energia elétrica;
b. falha de um elemento de conexão;
c. servidor fora do ar;
d. ausência de conexão com internet;
e. sabotagem / terrorismo;
f. indisponibilidade de acesso a Cooperativa;
g. ataques DDOS.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

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.

A Cooperativa deverá realizar as seguintes ações após a avaliação dos incidentes:

9.3.1. Avaliação Inicial

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.

9.3.2. Incidente Caracterizado

Caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

a. iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros;
b. o diretor responsável pela política de segurança cibernética avaliará o impacto do incidente nos diversos riscos envolvidos;
c. conforme a relevância (sabotagem, terrorismo etc.) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências;
d. conforme a relevância do incidente comunicar os associados que porventura tenham sido afetados;
e. comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela Coopernitro.

9.3.3. Recuperação

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

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

Coopernitro perdeu informações ou dados, a Diretoria Executiva e equipe de contingência deverão ser informados imediatamente.

9.3.4. Retomada

Na retomada dos processos, deverão ser definidos ações que devem incluir a análise e os procedimentos para que a Coopernitro possa operar normalmente, bem como reconstrução de eventuais sistemas e mudanças e medidas de prevenção.

9.4. MONITORAMENTO E TESTES

O ambiente de TI da Coopernitro deve ser supervisionado e monitorado com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, identificar possíveis anomalias, incluindo a presença de usuários, componentes ou dispositivos não autorizados. É possível a ocorrência de algum risco de segurança cibernética através de uma das seguintes situações descritas:

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.

A Coopernitro deve providenciar a execução de testes de cibersegurança através da verificação dos seguintes itens:

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;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

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 IT, com periocidade trimestral, elaborado a partir de suas políticas internas e as 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.

10. 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.

10.1. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES COM OUTRAS INSTITUIÇÕES

O “Compartilhamento de Informações sobre Incidentes Cibernéticos Relevantes” poderão ser realizadas por intermédio da Federação Nacional das Cooperativas de Crédito (FNCC_ por meio do registro Sistema Atendimento – Administrativo FNCC disponível no site https://fncc.com.br/.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

11. PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES RELEVANTES

Esta Política de Segurança Cibernética institui o Plano de Ação e de Respostas a Incidentes Relevantes com os seguintes objetivos:

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 ação abordará detalhadamente os cenários de incidentes a serem avaliados nos testes de continuidade de negócios, será aprovado pelo Diretor responsável pela Política de Cibernética e será revisado no mínimo anualmente.

12. RELATÓRIO ANUAL DE SEGURANÇA CIBERNÉTICA

A Coopernitro emitirá anualmente, com data base de 31 de dezembro, Relatório Anual de Segurança Cibernética referente a implementação do plano de ação e de respostas a incidentes relevantes.

Esse relatório deve ser elaborado até 31 de março do ano seguinte ao da data base, devendo ser aprovado pelo Diretor responsável pela Segurança Cibernética, e apresentado à Diretoria Executiva.

No relatório deverá contemplar, no mínimo, as seguintes informações:

a. a efetividade da implementação das ações relativas à Política de Segurança Cibernética;
b. o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
c. os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
d. os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

13. 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 a Diretoria Executiva, Conselho Fiscal, colaboradores, terceiros, e prestadores de serviços relevantes ou aqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados, do qual será evidenciada por meio de assinaturas nos Termo de Ciência;
b. divulgação no site aos associados e ao público, do resumo contendo as linhas gerais desta política.

14. 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 os 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.

15. DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL

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

a. Política de Segurança Cibernética;
b. Ata de Reunião da Diretoria Executiva com o registro referente a implantação e implementação a Política de Segurança Cibernética;
c. Documento relativo ao Plano de Ação e de Respostas a Incidentes Relevantes relativos à implementação da Política de Segurança Cibernética;

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

d. Relatório Anual de Segurança Cibernética sobre a implementação do Plano de Ação e de Respostas a Incidentes Relevantes;
e. Contratos e Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
f. Contratos e Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra;
g. 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.

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 comunicadas 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 Diretoria Executiva, Conselho Fiscal, colaboradores, terceiros, prestadores de

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

serviços relevantes, e aqueles 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.

São Paulo, 28 de agosto de 2025.

_____

Cláudio Nolasco
Presidente

_____

Eric Fernando Tomboly
Vice-Presidente

Clicksign dc93b549-6475-403b-b279-e6d5e64752f4

Política de Segurança Cibernética_versao06_28082025.pdf

Documento número #dc93b549-6475-403b-b279-e6d5e64752f4

Hash do documento original (SHA256): 2df0ff16d1bce4a725045bf70d1b105f20ce16ec7067362fa647e62eb0d082e5

Assinaturas

Eric Fernando Tomboly
CPF: 277.209.688-24
Assinou em 28 ago 2025 às 09:04:50

CLAUDIO NOLASCO
CPF: 006.053.628-40
Assinou em 28 ago 2025 às 10:49:03

Log

28 ago 2025, 08:59:13	Operador com email renata.paschoalato@coopernitro.com.br na Conta 9becfaed-5ed3-4403-b150-af1283761c67 criou este documento número dc93b549-6475-403b-b279-e6d5e64752f4. Data limite para assinatura do documento: 27 de setembro de 2025 (08:59). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
28 ago 2025, 08:59:58	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.
28 ago 2025, 08:59:58	Operador com email renata.paschoalato@coopernitro.com.br na Conta 9becfaed-5ed3-4403-b150-af1283761c67 adicionou à Lista de Assinatura: eric.tomboly@nitro.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.
28 ago 2025, 09:04:50	Eric Fernando Tomboly assinou. Pontos de autenticação: Token via E-mail eric.tomboly@nitro.com.br. CPF informado: 277.209.688-24. IP: 152.249.104.154. Localização compartilhada pelo dispositivo eletrônico: latitude -23.56946637609438 e longitude -46.68945718519998. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1289.0 disponibilizado em https://app.clicksign.com.
28 ago 2025, 10:49:03	CLAUDIO NOLASCO assinou. Pontos de autenticação: Token via E-mail claudionolasco@coopernitro.com.br. CPF informado: 006.053.628-40. IP: 189.29.151.236. Componente de assinatura versão 1.1289.0 disponibilizado em https://app.clicksign.com.

28 ago 2025, 10:49:08	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número dc93b549-6475-403b-b279-e6d5e64752f4.

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

Este Log é exclusivo e deve ser considerado parte do documento nº dc93b549-6475-403b-b279-e6d5e64752f4, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.