POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. INTRODUÇÃO

A **Política de Segurança da Informação** constitui uma declaração formal da **Cooperativa de Economia e Crédito Mútuo Aliança – Coopernitro** acerca de seu compromisso com a proteção das informações de sua propriedade, estabelecendo diretrizes corporativas que permitam aos colaboradores e associados seguirem padrões de comportamento relacionados à segurança, adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

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

A presente Política de Segurança da Informação tem como objetivo definir as diretrizes da que nortearão as normas e padrões que tratam a proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio em que ela esteja contida.

3. REGULAMENTAÇÃO

Esta política tem como guias principais os conceitos e orientações das Normas Técnicas ABNT ISO/IEC da família 27000, com suas alterações posteriores e as normativas do Banco Central do Brasil. Segue também a regulamentação da Lei 13.709/2018 Lei Geral de Proteção de Dados Pessoais – LGPD.

4. APLICABILIDADE

Esta política aplica-se todos os componentes da estrutura organizacional, sendo Diretoria Executiva, Conselho Fiscal, colaboradores, terceiros, prestadores de serviços relevantes, associados e aqueles que utilizam as informações constantes nos ativos da Cooperativa.

5. CONCEITOS

Para esta política definimos:

a. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
b. Ativo de Informação: os meios, os locais, os equipamentos e os sistemas de armazenamento, transmissão e processamento da informação, algo que tenha valor para a Cooperativa;
c. Autenticidade: propriedade pela qual se assegura que a informação foi produzida ou expedida, modificada ou destruída por uma pessoa natural, equipamento, sistema, órgão ou entidade;
d. Backup: é uma cópia de segurança dos seus dados (física ou em nuvem) de um dispositivo de armazenamento ou sistema;
e. Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizados nem credenciados;
f. Firewall: dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;
g. Incidente de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
h. Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, no sentido de preservar o valor que possuem para a Cooperativa.

6. RESPONSABILIDADES

É de responsabilidade da Diretoria Executiva, Conselho Fiscal, colaboradores, estagiários, terceiros, prestadores de serviços relevantes e visitantes, observarem e seguirem as diretrizes, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação.

Todas as atividades executadas na Coopernitro devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

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.

6.1. DIRETORIA EXECUTIVA

São responsabilidades da Diretoria Executiva*:*

a. aprovar as diretrizes desta Política de Segurança da Informação (PSI);
b. aprovar as exceções que não conflitem com as normas legais;
c. avaliar e aprovar o Plano de Continuidade de Negócios (PCN);
d. aprovar a homologação de hardware e software realizada pelo prestador de serviço responsável pela segurança da informação;
e. aprovar as requisições de aquisições de software e hardware;
f. estabelecer diretrizes para a gestão da segurança da informação;
g. aprovar o orçamento em atendimento aos projetos referente a segurança da informação.

6.2. COORDENAÇÃO

São responsabilidades da Coordenação:

a. aprovar em conjunto com a Diretoria Executiva as requisições de aquisições de software e hardware*;*
b. tomar conhecimento e apresentar a Diretoria Executiva os incidentes de segurança da informação e das ações adotadas para resolução dos problemas;
c. aprovar em conjunto com a Diretoria Executiva o registro de ocorrências referente a segurança da informação, do tratamento e documentação dos problemas ocorridos e ações realizadas;
d. estabelecer o orçamento em atendimento aos projetos referente a segurança da informação;
e. monitorar os serviços da empresa contratada, abrangendo custos, prazos e qualidade dos produtos entregues referentes a segurança da informação;
f. informar o prestador de serviço responsável pela segurança da informação a admissão de colaboradores para disponibilização de equipamentos e liberação dos acessos aos sistemas;
g. recolher assinatura nos termos de responsabilidade de uso de equipamentos de informática e termo de devolução e mantê-los arquivados;
h. informar o prestador de serviço responsável pela segurança da informação a demissão de colaboradores para recolhimento de equipamentos e encerramentos acessos aos sistemas.

6.3. PRESTADOR DE SERVIÇO RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO

São responsabilidades do prestador de serviço responsável pela segurança da informação:

a. garantir a integridade da rede da Cooperativa através do uso de *firewalls* e programas antivírus;
b. instalar e monitorar o *Firewall* e VPN;
c. garantir segurança nos e-mails e implantar antivírus;
d. monitorar o servidor de serviços de rede;
e. instalar softwares nas estações de trabalho desde que homologados pela Diretoria Executiva;
f. instalar e desinstalar qualquer software considerado nocivo à integridade da rede por meio chamado no sistema da TI;
g. orientar os colaboradores sobre os princípios e procedimentos de segurança da informação, para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas;
h. atender as demandas dos usurários da Cooperativa com relação dúvidas e ocorrências de segurança da informação.

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

Os critérios a seguir deverão ser cumpridos rigorosamente por todos os usuários:

a. responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
b. relatar prontamente ao prestador de serviço responsável pela segurança da informação qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, intercepção de mensagens eletrônicas, acesso indevido ou desnecessário a pastas e diretórios de rede, acesso indevido à internet;
c. relatar prontamente, quando identificado, quaisquer programas instalados sem conhecimento ao prestador de serviço responsável pela segurança da informação;

d. assegurar que as informações e dados de propriedade da Cooperativa não sejam disponibilizados a terceiros e nem discutidos em ambientes públicos ou em áreas expostas como transporte público, restaurantes, etc.

A informação é um dos principais patrimônios da Coopernitro, refere-se a um ativo com constantes ameaças e quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos**.** Portanto, a Política de Segurança da Informação torna-se alicerce dos esforços de proteção à informação da Coopernitro.
A segurança da informação são esforços contínuos para a proteção dos ativos de informação e para tanto, visa atingir os seguintes objetivos:

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 a todas as pessoas autorizadas a tratá-las.

Quaisquer informações geradas ou recebidas por colaboradores como resultado da atividade profissional pertence a referida instituição, sendo que as exceções devem ser explicitamente formalizadas em contrato entre as partes. Os equipamentos de informática, comunicação, sistemas e informações utilizados pelos colaboradores são destinados à realização de atividades profissionais, sendo o uso pessoal eventual permitido desde que não prejudique o desempenho dos sistemas e serviços.
A Coopernitro poderá monitorar e registrar o uso dos sistemas e serviços visando garantir a disponibilidade e segurança das informações utilizadas.
Esta política se aplica a todas as áreas da Coopernitro suas dependências e outras unidades que possam vir a ser constituídas.
Os colaboradores e prestadores de serviços, usando a infraestrutura de tecnologia, concedem sua conformidade absoluta com as políticas corporativas de tecnologia, incluindo, ilimitado, seu consentimento para investigações, leitura e / ou revisões que as áreas designadas fazem relativas às informações, dados, arquivos, conteúdo e mensagens que enviam, recebem, armazenam ou acesso, utilizando a infraestrutura de tecnologia da Coopernitro, incluindo informações, dados e documentos pessoais,

sujeito a restrições provenientes de legislação aplicável e com conformidade com as diretrizes de gestão de dados pessoais de acordo à legislação do país.

Os colaboradores devem consultar com o gestor/coordenador, quaisquer perguntas sobre o uso de qualquer componente da infraestrutura de tecnologia para fins pessoais.

Na Coopernitro é considerado “PROIBIDO” os serviços de e-mail, mensagem instantânea e internet, aplicações e infraestrutura como segue:

a. qualquer atividade que interfira com as funções ou demanda produtividade dos colaboradores da Coopernitro;
b. busca, acesso, consulta, publicação ou transferência de conteúdo que não cumpre o Código de Ética e de Conduta do negócio da Coopernitro;
c. uso do software ou acesso aos sites da internet para conseguir o anonimato nas atividades realizadas e / ou na transferência de informação da internet;
d. enviar mensagens, documentos ou bens da informação da Coopernitro, dos colaboradores, dos seus associados ou dos seus fornecedores, a sites ou contas pessoais ou públicos sem haver a devida autorização do gestor/coordenador;
e. uso de e-mail, mensagem instantânea e internet como mídia de comunicação oficial da Coopernitro por quem não está autorizado a fazer.

Em casos de violação desta política, a Coopernitro reserva o direito de restringir ou cancelar o acesso a qualquer serviço mensagens instantâneas, e-mail, mídia social ou página de internet, total ou parcialmente, como determinado pela área de segurança da informação.

Todas as conexões de rede de internet da Coopernitro dever ser feito por meio de mecanismos de segurança (*firewall*), filtro de conteúdo e registro de atividade, de acordo com as normas de tecnologia, todo tráfego de mensagens, dados ou informações, de ou para qualquer equipe que está conectada às redes da Coopernitro deve seguir por tais mecanismos, ou o equipamento que este conecte à rede da Coopernitro em nenhum evento deve ser simultaneamente conectada às redes de terceiros.

7. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

7.1. PROTEÇÃO DA INFORMAÇÃO

A informação é um importante ativo para a operação das atividades comerciais da Coopernitro e deve ser adequadamente manuseada e protegida e pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e meio da comunicação oral.

Toda a informação gerada ou desenvolvida nas dependências da Coopernitro constitui ativo essencial à condução de negócios, e em última análise, à sua existência e deve ser utilizada unicamente para a finalidade para a qual foi autorizada, independente da forma ou por meio pelo qual é compartilhada. É imprescindível estabelecer como diretriz fundamental a proteção de todas as informações pertencentes à Coopernitro, a fim de mitigar riscos e ameaças que possam comprometer a confidencialidade, integridade e disponibilidade desses dados.

7.2. CORREIO ELETRÔNICO

A Coopernitro através do pessoal designado, sem qualquer condição de privacidade para os colaboradores, podem monitorar, investigar, ler e / ou verificar toda a atividade que os colaboradores e sem limite as informações, dados, conteúdo e mensagens ou arquivos enviados, recebidos ou armazenados, assim como sites da internet que visita e as atividades que realiza, com o objetivo de garantir a integridade dos sistemas informação e redes, a qualidade de operação dos mesmos, verificando a conformidade com os termos de utilização dos sistemas apresentados nesta política e cumprimento de outras políticas da Coopernitro.

7.3. ACESSO À INTERNET

O acesso à internet deve ser utilizado para fins corporativos, enriquecimento intelectual ou como ferramenta de busca por conhecimento, visando buscar informações que possam contribuir para o desenvolvimento das atividades relacionadas a Cooperativa.

São permitidas o acesso à internet para fins pessoais (home *banking,* lojas virtuais e afins) desde que o colaborador tenha bom senso e respeitando os direcionamentos de segurança estabelecidos.

É VEDADO o uso da internet para acesso a sites de relacionamento qualquer tipo de *download* e *upload*, uso de softwares *"peer-to-peer" (*P2P) e acesso a computadores e acesso a site com conteúdo impróprios.

Os acessos externos à rede interna, para fins de manutenção de infraestrutura ou sistemas, somente poderão ser realizados através de empresas formalmente contratadas pela Coopernitro.

Os acessos à internet serão monitorados através de identificação do usuário, podendo ser bloqueados a qualquer momento pela equipe de tecnologia quando for identificado risco ao funcionamento do ambiente.

A estrutura de *firewalls* da empresa implementa o bloqueio de acesso a sites através do uso de *blacklists* de mercado. Qualquer exceção deve ser solicitada através de solicitação formal, identificando a exceção, o motivo e a vigência da liberação. A solicitação será analisada pelo gestor/coordenador.

7.4. CONTROLE DE ACESSO

A Coopernitro deverá manter restrito o acesso as áreas onde serão processadas ou armazenadas informações pertinentes à sua operação, mantendo lista de acesso a estes ambientes. O colaborador/usuário é responsável por todos os atos executados com suas credenciais de acesso, portanto deverá:

a. manter a confidencialidade, registrando as senhas em ambientes seguros;
b. alterar a senha sempre que existir qualquer suspeita de comprometimento de sua confidencialidade;
c. selecionar senhas de qualidades, cuidando para não usar informações pessoais, como datas de aniversários, entre outros;
d. evitar o uso dos equipamentos por outros colaboradores enquanto este estiver conectado com suas credenciais;
e. bloquear sempre o equipamento ao se ausentar da estação de trabalho;
f. estar proibido de compartilhar a sua senha, e proibido do uso de logins automáticos e recursos de memorização de senhas.

7.5. AUTENTICAÇÃO E SENHAS

Na Coopernitro é realizado a autenticação de senhas que visa a evitar o acesso não autorizado a dados pessoais. As pessoas não autorizadas são aquelas que não detêm

legitimidade legal, regulamentar ou estatutária para o tratamento de dados. Assim, a autenticação nos sistemas é realizada através de senha pessoal e intransferível, ou seja, de responsabilidade exclusiva do colaborador/usuário.

A Coopernitro implementa a rigidez de senha exigida pela regulação em seus sistemas nativos e nas ferramentas terceirizadas, sempre que possível.

Para os logins de colaboradores que possuem acesso a sistemas internos estabelece-se os requisitos mínimos de senha a seguir:

a. tamanho mínimo de 8 (oito) caracteres;
b. proibição de reuso das últimas 6 (seis) senhas utilizadas na alteração;
c. exigência de complexidade alta (maiúscula, minúscula, caracteres especiais e números;
d. expiração de senha a cada 90 (noventa) dias;
e. bloqueio de senha após 3 (três) tentativas erradas;
f. desbloqueio de senha somente por acesso administrativo;
g. armazenamento em banco de forma criptografada.

A senha deverá ser trocada, através de solicitação periódica do responsável pela segurança da informação, seguindo o padrão descrito no item anterior e ser alterada pelo colaborador/usuário sempre que existir suspeita de comprometimento de sua confidencialidade. O colaborador/usuário não deverá:

a. compartilhar seu equipamento com outros colaboradores/usuários enquanto estiver conectado com suas credenciais**;**
b. se ausentar da estação, sem antes bloquear o seu equipamento (Ctrl+Alt+Del);
c. transferir ou compartilhar senha com ninguém, ou seja, terminantemente proibido o compartilhamento de login.

Também não é permitido habilitar logins automáticos com recurso de memorização de senha. A criação/uso de logins genéricos deve ser evitada.

Os terceiros, fornecedores, prestadores de serviços, visitantes devem ter seus “Logins” diferentes dos colaboradores da Coopernitro.

A criação e bloqueio de logins são atribuições da equipe de tecnologia mediante fluxo aberto através de chamado aberto em ferramenta correspondente.

O fluxo compreende as seguintes etapas:

- solicitação da Cooperativa de admissão/demissão de colaboradores;

- ativação ou bloqueio do login do colaborador para acesso a rede, e-mail e demais plataformas integradas pela equipe de suporte de tecnologia;
- definição de acessos e permissão do colaborador pelo gestor/coordenador.

7.6. BACKUP

Todos os dados críticos da Coopernitro são guardados em estruturas remotas com monitoração e procedimentos regulares de restauração. Maiores detalhes podem ser obtidos na Política de Backup.

7.7. SOFTWARES

Na Coopernitro somente são permitidas as instalações de softwares homologados. Anualmente será realizado um inventário de software em todas as estações, sendo facultado a área de tecnologia a desinstalação de qualquer software não homologado sem aviso prévio ao colaborador. A presença de softwares não homologados será comunicada ao gestor/coordenador da área, que tomará as medidas cabíveis.

7.8. ANTIVÍRUS

Todos os equipamentos da Coopernitro, sejam eles servidores ou estações, devem possuir antivírus instalados e atualizados periodicamente.

7.9. CLASSIFICAÇÃO DOS DADOS

Os dados poderão ser classificados em:

a. público: quando o conteúdo puder ser distribuído a qualquer pessoa interna ou externa e for de conhecimento geral;
b. somente interno: conteúdo produzido pela Cooperativa para conhecimentos exclusivos dos colaboradores, terceiros, fornecedores e prestadores de serviços relevantes;
c. confidencial: conteúdo sensível e de acesso apenas a pessoas que devem conhecer o conteúdo.

O acesso aos dados somente será autorizado aos colaboradores/usuários que tiver necessidade de conhecer a respectiva informação.

7.10. CRIPTOGRAFIAS E CERTIFICADOS DIGITAIS

A guarda das chaves de criptografia para acessos aos recursos computacionais devem ser mantidas de forma segura, bem como o registro de todas as chaves de criptografia e certificados digitais existentes. Devem ter controles e documentação do processo de guarda, renovação, revogação e inutilização de certificados digitais.

7.11. TESTES DE INVASÃO

O prestador de serviço responsável pela segurança da informação executa periodicamente rotinas de testes de defesa contra possíveis ataques aos sistemas de informação, rotinas estas denominadas de *Penetration Test*. Estas rotinas são realizadas em sistemas e ambientes que sejam acessíveis via internet.

7.12. CONSCIENTIZAÇÃO E COMUNICAÇÃO

As informações sobre potenciais ameaças à integridade dos sistemas de informação são repassadas periodicamente a todos os colaboradores.

7.13. REDE WI-FI

A empresa implementa redes sem fios segregadas, sendo a rede “Visitantes” usada basicamente para acesso à internet, sem acesso à rede corporativa e com menor rigidez e robustez. A rede “Corporativa”, entretanto, tem acesso normal aos recursos da rede, exigindo liberação prévia do equipamento com a equipe de tecnologia.

7.14. ARMAZENAMENTO OU DESCARTE DE INFORMAÇÃO

Na Coopernitro tem as seguintes diretrizes com relação ao armazenamento e descarte de informações:

a. as informações confidenciais não devem ser deixadas à vista, seja em papel ou em quaisquer dispositivos eletrônicos;
b. ao usar uma impressora coletiva, recolher o documento impresso imediatamente;
c. os colaboradores ou terceiros, fornecedores e prestadores de serviços relevantes não devem discutir ou comentar assuntos confidenciais em locais públicos.

7.15. EQUIPAMENTOS PARTICULARES/PRIVADOS

Os equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Coopernitro.

8. DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para uniformidade da informação, esta Política deve ser divulgada no âmbito da Coopernitro, tão logo aprovada pela Diretoria Executiva, seja na sua constituição ou em quaisquer atualizações que se façam necessárias. Adicionalmente deve ser disponibilizada, permitindo fácil acesso ou consulta a qualquer colaborador/usuário.

Esta Política também deve ser divulgada para novos colaboradores, no processo de integração. Os colaboradores, ao receberem os equipamentos de trabalho (computador/notebook), deverão assinar o termo de responsabilidade de uso de equipamentos de informática se responsabilizando pelo uso do hardware e software conforme esta Política de Segurança da Informação.

9. VIOLAÇÕES DA POLÍTICA E SANÇÕES

O descumprimento das diretrizes desta política, mesmo que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

É dever de todo colaborador comunicar ao gestor/coordenador a ocorrência de incidente que afete a segurança da informação, que por sua vez escalará a Diretoria Executiva para análise quando assim for necessário.

10. POLÍTICA INTERNA DE PRIVACIDADE DE 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 – Coopernitro, a qual dispõe sobre o tratamento de dados em observância a Lei nº 13.709/2018 (LGPD).

11. 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.

12. CONSIDERAÇÕES FINAIS

A Diretoria Executiva compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta política.

O cumprimento desta Política de Segurança da Informação é de responsabilidade Diretoria Executiva, Conselho Fiscal, colaboradores, terceiros, fornecedores e prestadores de serviços relevantes e aqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados.

Os colaboradores/usuários estão proibidos de acessar informações da Coopernitro que não sejam explicitamente autorizados. Os indícios ou irregularidades devem ser comunicadas ao prestador de serviço e ao diretor responsável pela segurança da informação.

A presente política poderá ser alterada sem prévio aviso em virtude de alterações legislativas. Todas as observações e ocorrências, assim como ações a serem aprimoradas para atualização, 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

Política de Segurança da Informação_versao05_28082025.pdf

Documento número #8478d272-85af-446d-8378-f42ed3526495

Hash do documento original (SHA256): dae1900d9cf9896321ad07ef4c41e33d0e819ff46d1a0de121578d08620c2b33

Assinaturas

CLAUDIO NOLASCO
CPF: 006.053.628-40
Assinou em 28 ago 2025 às 10:49:57

Eric Fernando Tomboly
CPF: 277.209.688-24
Assinou em 28 ago 2025 às 09:05:20

Log

28 ago 2025, 09:00:24	Operador com email renata.paschoalato@coopernitro.com.br na Conta 9becfaed-5ed3-4403-b150-af1283761c67 criou este documento número 8478d272-85af-446d-8378-f42ed3526495. Data limite para assinatura do documento: 27 de setembro de 2025 (09:00). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
28 ago 2025, 09:00:52	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, 09:00:52	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, 09:05:20	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, 10:49:57	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, 10:49:59	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 8478d272-85af-446d-8378-f42ed3526495.

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