CREDCOL
COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO
DOS EMPREGADOS DO GRUPO colorado

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

Esta Política de Segurança Cibernética tem como objetivo assegurar a proteção dos ativos de informação da Cooperativa de Economia e Crédito Mútuo dos Empregados do Grupo Colorado 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 cooperados.

2. APLICABILIDADE

Esta política aplica-se a Diretoria Executiva, Conselho Fiscal, empregados, terceiros (fornecedores e prestadores de serviços) e aqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados.

3. DEFINIÇÃO

Para esta política definimos:

a) segurança cibernética: é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e 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) risco cibernético: ameaça à confidencialidade, integridade e disponibilidade das informações.

e) 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 cooperados e componentes físicos, como servidores, estações de trabalho, notebooks etc.;

4. RESPONSABILIDADES

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

4.1. DIRETORIA EXECUTIVA

São responsabilidades Diretoria Executiva:

a) aprovar esta Política de Segurança Cibernética, o plano de ação e de respostas de incidentes relevantes e o relatório anual 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 os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança cibernética.

4.2. 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;

b) acompanhar se as diretrizes da política estão sendo executadas;

c) executar o plano de ação e de respostas de incidentes e respostas a incidentes relevantes;

d) elaborar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes.

4.3. GERÊNCIA

São responsabilidades Gerência

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 empregados apenas quando forem realmente necessários.

4.4. ÁREA RESPONSÁVEL PELA SEGURANÇA CIBERNÉTICA

São competências da área 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) propor projetos e iniciativas para melhoria do nível de segurança cibernética da Cooperativa;

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;

h) 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;

i) informar ao BCB sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem;

j) comunicar ao BCB as providencias tomadas para reinício das atividades após a interrupções dos serviços na Cooperativa.

4.5. DEMAIS INTEGRANTES COM ACESSO AOS DADO OU SISTEMAS UTILIZADOS PELA COOPERATIVA

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

a) notificar a Diretoria Executiva dos 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;

5. PRINCÍPIOS E PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

Na implementação desta política considera o porte, perfil de risco, modelos dos negócios, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais da Cooperativa.

Considera-se a sensibilidade dos dados e informações que estão sob as responsabilidades da Cooperativa.

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.

5.1. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações serão classificadas considerando a relevância, sensibilidade, criticidade e grau de sigilo para os negócios e 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 Cooperativa e que estão disponíveis para todos os empregados;

c) **restrita**: são informações disponíveis apenas aos empregados específicos da Cooperativa, que as necessitem para exercer suas atribuições;

d) **confidencial:** são informações sigilosas de caráter estratégico para a Cooperativa e que estão disponíveis somente para Diretoria Executiva e pessoas por ela autorizadas.

5.2. PROCEDIMENTOS DE CONTROLES DOS EMPREGADOS

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

Todos os empregados 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 a as diretrizes de segurança da informação aprovada pela Cooperativa.

Quaisquer riscos às informações relacionados ao ambiente cibernético da Cooperativa devem ser comunicados diretamente a Diretoria Executiva por e-mail ou através dos canais de atendimento

5.3. AVALIAÇÃO DA RELAVÂNCIA DOS INCIDENTES

Os critérios a serem utilizados na avaliação da relevância dos incidentes na Cooperativa 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.

5.4. PROCEDIMENTOS DE CONTROLES

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

a) autenticação;

b) criptografia;

c) prevenção e detecção de intrusos;

d) prevenção de vazamento de informações;

e) 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) backup dos dados e das informações

5.5. 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 Cooperativa, 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 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 Cooperativa faz verificação da capacidade potencial do prestador de serviços a fim de assegurar o cumprimento da legislação em vigor, permissão de acessos da Cooperativa aos dados e as informações que serão processadas ou armazenadas.

O prestador de serviços deve manter a confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas e armazenadas.

A Cooperativa 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.

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.

Ainda, 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.

5.5.1. 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 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 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 (BCB):

a) a obrigação de a 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; e

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 trinta dias de antecedência da data prevista para a interrupção, observado que:

I. a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

II. a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

5.5.2. COMUNICAÇÃO AO BANCO CENTRAL DO BRASIL

A Cooperativa 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 10 (dez) dias após a contratação dos serviços e deve conter as seguintes informações:

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 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 Cooperativa, deve observar os seguintes requisitos:

a) existência de convênio para troca de informações entre o BCB 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 BCB;

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 Cooperativa deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A Cooperativa 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 BCB aos dados e às informações.

5.6. PLANO DE AÇÃO E RESPOSTAS A INCIDENTES

Esta Política de Segurança Cibernética institui o Plano de Ação **(Anexo I)** e de Relatório de Respostas a Incidentes Relevantes **(Anexo II)** 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, considerando a avaliação de risco dos incidentes por níveis de impacto nos negócios, sendo esses níveis estipulados em gravíssimo, grave, médio, baixo e muito baixo.

5.7. 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/.

6. PROTEÇÃO E PREVENÇÃO DE RISCOS CIBERNÉTICO

As ações de proteção e prevenção da Cooperativa 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 não autorizados ou software não licenciado;

c) manter os sistemas operacionais e software atualizados;

d) realizar frequentemente testes de invasão externa e pishing;

e) fazer análises de vulnerabilidade na estrutura tecnológica da Cooperativa frequentemente ou em situações que houver mudança significativas;

f) fazer teste do plano de resposta a incidentes com simulação de cenários.

7. TRATAMENTO DE INCIDENTES

Os incidentes são interrupções de sistema tecnológico não planejados que afetam os negócios da Cooperativa e podem acontecer nas seguintes situações:

a) queda de energia;

b) falha de um elemento de conexão ou servidor fora do ar;

c) ausência de conexão com a internet;

d) terrorismo;

e) ataques de DDOS;

f) indisponibilidade de acesso a Cooperativa.

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:

a) avaliar o impacto dos incidentes na Cooperativa;

b) redirecionar as linhas de telefones para os celulares, instruir o provedor de telefonia a desviar linhas de dados, entre outros;

c) avaliar a relevância, em caso de sabotagem ou terrorismo, a fim de decidir pelo registro de boletim de ocorrência ou outras providencias caso seja necessário;

d) comunicar tempestivamente ao Banco Central do Brasil as ocorrências de incidentes relevantes e as interrupções de serviços relevantes que configurem uma situação de crise na Cooperativa.

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 Cooperativa perdeu informações ou dados**,** a Diretoria Executiva e equipe de contingência devem ser informados imediatamente e na retomada dos processos deverão ser definidos ações que devem incluem a análise e procedimentos para que a Cooperativa possa operar normalmente, bem como reconstrução de eventuais sistemas e mudanças e medidas de prevenção.

8. DISSMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

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

a) promover programas de capacitação e avaliação periódica de todos os empregados;

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.

9. RELATÓRIO ANUAL DE SEGURANÇA CIBERNÉTICA SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES

A Cooperativa 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 **(Anexo III)**

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.

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

a) efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética;

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

c) incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

d) resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

10. DIVULGAÇÃO DA POLÍTICA DE SEGURANAÇA CIBERNETICA

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

a) divulgação desta política a Diretoria Executiva, Conselheiro Fiscal, empregados, associados, terceiros (fornecedores e prestadores de serviços) ou aqueles que tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados;

b) divulgação ao público, no site da Cooperativa;

11. 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 Diretoria Executiva com o registro referente a implantação e implementação a Política de Segurança Cibernética;

b) documento relativo ao plano de ação e de resposta a incidentes relativos à implementação da Política de Segurança Cibernética;

c) relatório anual sobrea implementação do plano de ação e de resposta a incidentes;

d) documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem; ***(se houver);***

e) documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra; ***(se houver)***

f) contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem*;* ***(se houver)***

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 resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. ***(se houver)***

12. TREINAMENTO

A Cooperativa estabelece, anualmente, um programa de conscientização em segurança cibernética para para empregados, com a finalidade de garantir que os objetivos e diretrizes definidos nesta política sejam cumpridos e apresentar às necessidades e responsabilidades específicas de cada empregado.

13. ATENDIMENTO A LEI Nº 13.709/2018

Todos os procedimentos e diretrizes desta política são realizados em conformidade e observância a Lei nº 13.709/2018 (LGPD).

14. PERIODICIDADE DE REVISÃO

Esta Política será revisada a cada 02 anos pela Diretoria Executiva**,** em decorrência de apontamentos de auditorias ou mudanças nas regulamentações.

15. CONSIDERAÇÕES FINAIS

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

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

16. APROVAÇÃO

Este normativo foi aprovado na reunião da Diretoria Executiva realizada em ***22/08/2025***conforme Ata de Reunião nº ***07/2025*** e passa a vigorar na data de sua publicação.

17. ANEXOS (MODELOS DE RELATÓRIOS) SUPORTE

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

18. REFERÊNCIAS NORMATIVAS

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. ***(Revogado pela Resolução CMN nº 4.893/2021).***
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.

19. CONTROLES DE ATUALIZAÇÕES

Edição	Data	Instrumento de atualização	Atualizações

Valter Marcos Lorenti – Diretor Presidente

Eli Norberto Ferreira – Diretor Tesoureiro

José Antônio Pimenta – Diretor Secretário

Página de assinaturas

Valter Lorenti
442.363.368-04
Signatário

eli ferreira
041.239.898-29
Signatário

HISTÓRICO

21 ago 2025 10:27:08 — **CREDCOL COOPERATIVA** criou este documento. (Empresa: CREDCOL, CNPJ: 02.024.442/0001-01, Email: credcolcolorado@gmail.com, CPF: 325.343.978-00)

21 ago 2025 10:29:32 — **Valter Marcos Lorenti** *(Email: valter.lorenti@colorado.com.br, CPF: 442.363.368-04)* visualizou este documento por meio do IP 177.200.72.34 localizado em Ribeirão Preto - São Paulo - Brazil

21 ago 2025 10:29:37 — **Valter Marcos Lorenti** *(Email: valter.lorenti@colorado.com.br, CPF: 442.363.368-04)* assinou este documento por meio do IP 177.200.72.34 localizado em Ribeirão Preto - São Paulo - Brazil

21 ago 2025 12:05:32 — **eli norberto ferreira** *(Email: eli.ferreira@colorado.com.br, CPF: 041.239.898-29)* visualizou este documento por meio do IP 177.21.47.210 localizado em Itajobi - São Paulo - Brazil

21 ago 2025 14:17:11 — **eli norberto ferreira** *(Email: eli.ferreira@colorado.com.br, CPF: 041.239.898-29)* assinou este documento por meio do IP 177.21.47.210 localizado em Itajobi - São Paulo - Brazil