

**CoopCREDER** Cooperativa de Economia e Crédito Mútuo  
dos Colaboradores da Coopeder Ltda.

# CoopCREDER

## Política de Segurança Cibernética



## **Introdução**

A Resolução CMN nº 4.658/2018, revogada pela Resolução CMN nº 4.893, de 26 de fevereiro de 2021, dispõe sobre a Política de Segurança Cibernética e sobre os requisitos necessários para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, os quais deverão ser observados pela CoopCREDER.

A Política de Segurança Cibernética deve ter o propósito de estabelecer requisitos que deverão ser observados tanto para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, quanto para o acesso dos colaboradores da empresa responsável pelo software utilizado pela CoopCREDER, além dos próprios colaboradores da Instituição.

Ressalta-se que, a descrição da Política de Segurança Cibernética, além de definir os procedimentos e mecanismos relacionados com a segurança das informações, tendo em vista os serviços terceirizados da área de informática e que se encontram em Nuvem, visa garantir através da segurança e confiabilidade a continuidade da Cooperativa, quando busca minimizar os riscos que porventura a instituição possa estar exposta.

Não obstante, caberá ao Conselho de Administração, no uso de suas atribuições conferidas no Estatuto Social, que sejam os responsáveis pelo gerenciamento da Política de Segurança Cibernética.

## **Da Implementação**

A Política de Segurança Cibernética da CoopCREDER foi formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, sendo compatível com:





- o porte, o perfil de risco e o modelo de negócio da instituição;
- a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e
- a sensibilidade dos dados e das informações sob responsabilidade da instituição.

### **Dos Conceitos**

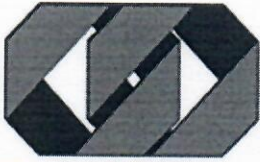
Para melhor compreensão da necessidade de se cumprir o descrito numa Política de Segurança Cibernética, é necessário conhecer os conceitos que fazem parte desse segmento, onde a informação é extremamente valiosa e passível de riscos que colocam em xeque a continuidade da instituição. Dessa forma, tem-se os seguintes conceitos para facilitar o entendimento dos colaboradores:

Segurança Cibernética: refere-se a um conjunto de práticas adotadas pelas instituições, que protege a informação armazenada nos computadores e aparelhos de computação, cujo fluxo se dá através de redes de comunicação em nuvem. Essa proteção visa garantir a propriedade da informação quanto a sua confidencialidade, integridade e disponibilidade.

Informação: é a reunião ou conjunto de dados e conhecimentos organizados, que possam constituir referências sobre determinado acontecimento ou processos comunicativos;

Confidencialidade: considera-se que, toda informação deve ser protegida, principalmente se considerado suas características e o grau de sigilo, de forma que exista limitação de acesso e uso apenas às pessoas autorizadas ou a quem é destinada;

Integridade: toda informação deve ser mantida na condição em que foi disponibilizada pelo seu titular, visando protegê-la contra alterações indevidas, intencionais e acidentais;



Disponibilidade: toda informação gerada ou adquirida por um indivíduo ou instituição, deve estar disponível aos seus usuários quando estes necessitarem delas para qualquer finalidade;

Riscos Cibernéticos: são considerados ataques que as informações podem sofrer, oriundos de malware, invasões, fraudes externas, desprotegendo, inclusive, redes e sistemas das empresas, podendo causar danos financeiros, à reputação, e até mesmo colocar em risco a continuidade da instituição;

#### Malwares

Vírus: software que causa danos à máquina, rede, softwares e banco de dados;  
Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

Spyware: software malicioso para coletar e monitorar o uso de informações;

Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja restabelecido;

Pharming: direciona o usuário para um site fraudulento, sem seu conhecimento;

Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável, que envia comunicação eletrônica oficial para obter informações confidenciais;

Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;





Acesso Pessoal: pessoas localizadas em lugares públicos como: bares, cafés e restaurantes, que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque;

Fraudes Externas e Invasões: realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico; e

Ataque DDoS e Botnets: ataques que visam negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de inúmeros computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação do serviço.

### **Dos Objetivos**

Atualmente, as discussões existentes nas áreas de tecnologia e segurança da informação, versam sobre a tendência da chamada cloud computing, ou seja, a computação em nuvem.

A computação em nuvem é a possibilidade de acesso ao banco de dados contendo as informações da instituição, em um ambiente externo, em outros servidores cuja infraestrutura e administração não serão mais de responsabilidade da instituição.

Se sob uma ótica apresenta-se com vantagens que vão desde flexibilidade, economia de escala, visto que transfere para outro os investimentos e custos para manutenção e atualizações, por outro, passam-se a existir uma série de preocupações sobre a segurança, visto que, quanto maior o fluxo de dados transferidos para a nuvem, proporcionalmente crescerá o comprometimento desses dados pessoais e privados.

Uma das premissas para viabilização da computação em nuvem é a virtualização, que requer muitas preocupações com a segurança, principalmente





no modelo de serviço contratado. Significa que, envolverá questões jurídica-contratual, responsabilizações por falhas ou problemas, devendo ser avaliados os aspectos relacionados à contratação, treinamentos e aperfeiçoamento de empregados das empresas prestadoras de serviço.

Se por um lado a virtualização pode oferecer risco, ela também se apresenta como opção de ganho de escala. Uma vez que se contrate um Cloud Service Provider – CSP, ou seja, Provedor de Serviços em Nuvem, este possui escala para ter em seu quadro funcional profissionais capacitados e qualificados em maior quantidade do que nas pequenas e médias empresas, o que conta como fator positivo para adoção da computação em nuvem.

### **Requisitos para Contratação de Serviços de Processamento e Armazenamento em NUVEM**

A CoopCREDER, tendo em vista o seu porte, o perfil de risco que encontra-se exposta, bem como o modelo de negócio adotado, deve observar os seguintes requisitos quando da contratação de serviços de processamento e armazenamento de dados em nuvem:

- Verificar se, a empresa contratada adota práticas de governança corporativa e de gestão, proporcionais à relevância do serviço contratado e aos riscos a que estejam expostas;
- Verificar a capacidade potencial do prestador de serviço de assegurar o cumprimento da legislação e da regulamentação em vigor;
- Verificar a capacidade potencial do prestador de serviço de assegurar o acesso da instituição aos dados e às informações a serem processadas ou armazenadas pelo prestador;
- Verificar a capacidade potencial do prestador de serviço de assegurar a confiabilidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço;





- Verificar a capacidade potencial do prestador de serviço de assegurar a sua aderência a certificações exigidas pela instituição para prestação do serviço contratado;
- Verificar a capacidade potencial do prestador de serviço de assegurar o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- Verificar a capacidade potencial do prestador de serviço de assegurar o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- Verificar a capacidade potencial do prestador de serviço de assegurar a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos e lógicos; e
- Verificar a capacidade potencial do prestador de serviço de assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Para que a Política de Segurança Cibernética atinja seu propósito é imprescindível a participação dos colaboradores da Cooperativa na internalização dos seguintes requisitos:

- Zelar pela reputação da Instituição como forma de garantir a sua importância junto ao segmento que esta encontra inserida;
- Garantir que os princípios da confidencialidade, integridade e disponibilidade das informações da CoopCREDER e de seus respectivos cooperados, sejam protegidos contra acessos indevidos, alterações e modificações não autorizadas, sem que isso afete o acesso à informação por parte de quem possui permissão e/ou autorização;
- Garantir a operacionalidade das atividades da CoopCREDER, protegendo-a de interrupções causadas por falhas humanas internas;

*(Handwritten signature and initials)*





- Acatar aos requisitos legais, tanto os regulamentares quanto às obrigações contratuais pertinentes às atividades exercidas pela CoopCREDER;
- Promover a conscientização, educação e treinamento dos colaboradores por meio da Política de Segurança Cibernética, disponibilizando cursos, treinamentos, e demais procedimentos internos que norteiam suas atividades;
- Buscar a melhoria contínua dos processos que possam gerir os riscos de segurança Cibernética; e
- Seguir as orientações e realizar os procedimentos orientados pela empresa responsável pelo Serviço de Computação em Nuvem.

### **Diretrizes Corporativas**

A Política de Segurança Cibernética no que concerne a manutenção, atualizações, monitoramento e realização de testes, será norteada por diretrizes definidas pela PRODAF INFORMÁTICA que deverá informar a CoopCREDER sobre os procedimentos realizados e as conclusões obtidas através de relatórios e/ou declarações.

Sendo assim, as diretrizes definidas pela PRODAF INFORMÁTICA encontram-se assim definidas:

- Realizar diariamente testes no sistema de forma a verificar sua acessibilidade e usabilidade;
- Realizar pentests para mostrar/detectar eventuais vulnerabilidades;
- Acompanhar em tempo real, através de ferramenta automatizada de monitoramento de ambientes, as questões relacionadas a cargas e desempenho, onde são gerados alertas em caso de pico de uso de recurso de algum servidor;
- A PRODAF INFORMÁTICA é a responsável em administrar e verificar o banco de dados que pode ser executada de forma manual ou automática;
- Proceder com a monitoração automática do ambiente de produção; e
- Realizar backups.





Tendo em vista o previsto na Resolução CMN nº 4.893/2021, os serviços de computação em nuvem abrangem a disponibilidade à instituição contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamentos de dados, infraestrutura de redes e outros recursos computacionais, que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviço; e
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

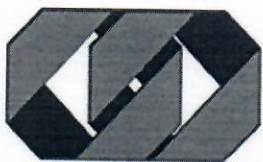
### **Contratação dos Serviços de Processamento e Armazenamento de Dados em NUVEM**

A CoopCREDER, tendo em vista a necessidade de otimizar o atendimento de seus cooperados e visando maior segurança e celeridade, fez a contratação do Serviço de Computação em Nuvem.

O contrato foi firmado com a empresa PRODAF INFORMÁTICA que, é a responsável pelos serviços de processamento e armazenamento de dados conforme disposto na Resolução nº 4.893, de 26 de fevereiro de 2021. Esta, por sua vez, possui contrato regular de Serviços junto a DEDALUS que, é detentora do espaço utilizado pela CoopCREDER para armazenar seus dados.

Por sua vez, o espaço objeto do contrato entre a DEDALUS x PRODAF INFORMÁTICA pertence à AMAZON WEB SERVICES, conforme Termo de Adesão de Proposta Comercial 2850A.14, datado de 15/08/2014, onde foram escolhidas as seguintes opções de serviços: **Serviços de Hospedagem AWS**





**– Franquia Mensal e Serviço de Suporte DEDALUS – Nível de Serviços Enterprise.**

De acordo com o ANEXO I – Níveis de Serviços DEDALUS Infrastructure as a Service - IaaS – disponibilizado para Coopermc, o **Nível de Serviços Enterprise** destina-se a projetos críticos para o cliente, tais como sistema ERP, e-commerce ou ambiente web de alto impacto no negócio. Cabe a DEDALUS a responsabilidade por toda a sustentação do ambiente, seu crescimento, contingência da infraestrutura IaaS, análise integrada de mudança, atendimento personalizado etc. Tarefas como: administração, backup, monitoramento, entre outros, passam a ter uma dimensão típica de ambientes de missão crítica.

**Acompanhamento e Controle**

Os procedimentos e as instruções encontram-se presentes na Política de Segurança Cibernética, visto que, estes representam as responsabilidades atribuídas à PRODAF INFORMÁTICA, por conta do objeto do contrato de Serviço de Computação em Nuvem.

Assim, é necessário um acompanhamento e controle das ações, as atividades desenvolvidas e a sua relação com as informações. Esse nível de detalhamento pressupõe a necessidade de constante revisão e/ou manutenção dessa política, conforme a seguir:

Testes

São realizados testes, sendo estes executados de forma automatizada e por robôs de monitoramento, diariamente.

Acompanhamento

O acompanhamento de carga e desempenho é realizado em tempo real, através de ferramenta automatizada que, no processo de monitoramento do ambiente, pode gerar alertas em caso de pico de uso e recurso de algum servidor.





#### Administração do Banco de Dados

Toda a parte de administração e verificação do banco de dados é de exclusiva responsabilidade da PRODAF INFORMÁTICA, sendo operacionalizada de forma manual ou automática pelas versões do sistema.

#### Administração de Contas de Usuários

Os usuários que utilizam o SYSCOOP32, serão geridos e autorizados pela CoopCREDER. Já o cadastro e criação de usuários para acessar o Cloud pelo GO-Global, será realizado pela PRODAF INFORMÁTICA mediante solicitação da Instituição.

#### Administração de Ferramentas de Segurança

A administração das ferramentas de segurança como firewalls, IDS/IPS e WAF, serão de responsabilidade da PRODAF INFORMATICA e da DEDALUS. Há um monitoramento constante de ocorrências e aplicação de vacinas e regras que visam evitar problemas com ataques.

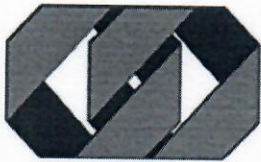
#### Plano de Contingência

Como todo o ambiente PRODAF INFORMÁTICA cloud é virtualizado, a qualquer momento, sendo necessário, podem-se levar os snapshots dos servidores para qualquer datacenter da AMAZON no mundo, de forma a subir um novo ambiente de uso dos sistemas. Para acesso às informações, basta o funcionário CoopCREDER autorizado, conectar-se a qualquer rede de internet, em qualquer lugar do mundo.

#### Ocorrência de Incidente

As verificações são realizadas por meio de pentests, que tem ocorrido de acordo com demanda dos clientes e com certa frequência.

O tempo de restabelecimento por um eventual ataque, uma vez ocorrendo, dependerá do tipo de ataque, visto que, eventualmente, pode ser resolvido em



poucos minutos ou, havendo situações mais complexas, demandará a abertura de uma janela maior para correção. No pior dos cenários, o retorno de snapshot pode ocorrer no máximo em 02 (duas) horas.

### **Registros de Incidentes**

Considerando a responsabilidade da PRODAF INFORMÁTICA na administração do banco de dados e das ferramentas de segurança da CoopCREDER, torna-se necessário a comunicação à Conselho de Administração de qualquer incidente relevante, sendo formalizado através de relatório e/ou declaração contendo o registro dos Incidentes verificados em testes, ou os que efetivamente ocorreram, considerando as seguintes situações:

- Validação dos procedimentos internos;
- Validação dos controles de tecnologia;
- Informações detalhadas dos incidentes considerados relevantes relacionados com o ambiente cibernético;
- Informações sobre a forma de mitigação das ocorrências relevantes; e
- Resultados dos testes do ambiente.

### **Responsabilidades entre DEDALUS X PRODAF INFORMÁTICA**

#### **DEDALUS**

##### ***Licenciamento de Software***

- Licença de sistemas operacionais;
- Licença do banco de dados;
- Licença do software antivírus; e
- Licenciamento dos softwares de monitoramento e backup.

##### ***Instalação e Configuração do Ambiente***

- Instalação/Configuração do Sistema Operacional e pacotes corretivos;
- Instalação do Sistema Gerenciador de Banco de Dados (SGBD) e pacotes corretivos;





- Instalação dos agentes de monitoramento do ambiente;
- Configuração dos serviços de DNS (Route 53/ Azure DNS);
- Configuração das regras de Firewall (AWS/ Azure);
- Configurações de acesso FTP;
- Configurações do ambiente de Backup; e
- Operação de Snapshot.

### **Administração do Ambiente**

- Acesso ao painel administrativo (AWS/Azure);
  - Gerenciamento de Infraestrutura;
  - Responsabilidade pelo gerenciamento dos dados do ambiente;
  - Administração e serviços (AWS/Azure);
  - Administração de Sistema Operacional;
  - Administração e suporte ao banco de dados;
  - Evolução do Banco de Dados;
  - Administração do Firewall (AWS/ Azure);
  - Operação de backup e restore de dados;
  - Administração do software antivírus e configuração das políticas;
- 
- Equipe de operação e monitoramento em formato 24 x 7;
  - Análise de vulnerabilidades;
  - Relatório de performance IaaS; e
  - Execução de Integração Contínua (continuous delivery);

### **Suporte**

- Ferramenta para abertura de chamados em regime 24 x 7, com tempo de resposta conforme níveis de serviço contratado;
- Operação 24 x 7

## **PRODAF INFORMÁTICA**

### **Licenciamento de Software**

- Licenças de Aplicativos que não fazem parte do contrato firmado entre PRODAF X DEDALUS e que serão de uso e/ou interesse daquela;



- Licenciamento e configuração de Certificados Digitais; e
- “Upgraed” de software em função de necessidade do Cliente.

### ***Instalação e Configuração do Ambiente***

- Instalação/ Configuração das aplicações;
- Configuração do banco de dados;
- Informar e responsabilizar procedimentos de configuração do banco de dados;
- Informar os domínios e entradas DNS a serem hospedados;
- Informar regras de firewall necessárias para funcionalidade do ambiente;
- Instalação e Configuração dos Softwares não descritos em propostas;
- Upload dos arquivos e base de dados;
- Validação do pleno funcionamento das aplicações com o ambiente sugerido em proposta;
- Configuração de acesso VPN (rede local); e
- Disponibilização de janelas para execução de mudanças.

### ***Administração do Ambiente***

- Responsabilidade pelos conteúdos e dados armazenados;
- Gestão e Governança do Parceiro;
- Gerenciamento de Performance das aplicações;
- Operações e Suporte às aplicações;
- Gerenciamento de código-fonte; e
- Gerenciamento de segurança das aplicações.

### ***Suporte***

- Atendimento de chamados para aplicações de Terceiros ou Proprietárias.

### **Do Gerenciamento**

Embora a responsabilidade pela administração do banco de dados, bem como das ferramentas utilizadas para garantir a segurança desses dados, seja de





responsabilidade da PRODAF INFORMÁTICA, a CoopCREDER deve garantir, como parte interessada, e se respaldar do atendimento da Política de Segurança Cibernética por parte daquela, através de relatórios e/ou declarações emitidos por conta da verificação dos controles de Segurança Cibernética, cuja periodicidade deve ser semestral.

Esse gerenciamento dos procedimentos e controles tem o objetivo de assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e modificados de acordo com os objetivos e diretrizes estabelecidas na Política de Segurança Cibernética da CoopCREDER.

Nesse sentido, a estrutura de gerenciamento deve prever o atendimento de padrão mínimo para conhecimento da Conselho de Administração da Instituição.

### **1 - Gestão de acesso às informações**

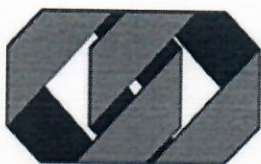
O acesso e cadastro de usuários para acessar o Cloud pela GO-Global serão realizadas pela PRODAF INFORMÁTICA mediante solicitação da Instituição. Nesse sentido, caberá a esta a verificação do controle de acessos, por conta do monitoramento efetivado, que devem ser revistos periodicamente como forma de manter as restrições e/ou permissões autorizadas pela Instituição.

### **2 - Proteção do Ambiente**

Considerando os serviços contratados de processamento e armazenamento em nuvem, torna-se prudente a apresentação de relatórios que demonstrem o efetivo monitoramento, aplicação de testes, tratamentos e resposta aos incidentes, quando de sua ocorrência, com vistas a minimizar o risco de falhas, favorecendo uma administração segura e transparente para ambas as partes. Esse relatório deve ser apresentado ao Conselho de Administração da CoopCREDER anualmente.

### **3 - Segurança Física e Lógica**





Caberá à PRODAF INFORMÁTICA orientar se as condições e configurações das máquinas utilizadas pela CoopCREDER, atendem aos propósitos estabelecidos para o bom desempenho e gerenciamento do serviço em nuvem.

No que tange ao seu quadro de colaboradores, a PRODAF INFORMÁTICA deve mantê-los atualizados e em constante treinamento, com vista a acompanhar as novidades acerca da Segurança da Informação e Cibernética.

#### ***4 - Continuidade de Negócio***

A estrutura de gerenciamento, em linhas gerais, visa garantir que a Política da Informação está sendo cumprida, com vistas a minimizar a ocorrência de fatores que coloquem em risco as atividades da CoopCREDER, e conseqüentemente expondo-a a risco de descontinuidade.

Nesse sentido, para evitar a descontinuidade do negócio, torna-se necessário proceder com a análise dos incidentes, de forma que estes correspondam a um nível crítico ou aceitável, e verificar se estão em consonância com as medidas corretivas a serem adotadas.

#### ***5- Reporte / Comunicação ao Conselho de Administração***

Tendo em vista a complexidade que envolve o cumprimento da Política de Segurança Cibernética, e a dificuldade da CoopCREDER em validar ou não a efetivação dos procedimentos, é imperioso manter a Conselho de Administração informada sobre indícios de irregularidades verificados quando do cumprimento das determinações dessa política.

Assim, caberá à PRODAF INFORMÁTICA realizar a comunicação de possíveis indícios quando de sua ocorrência ou, semestralmente, quando encaminhar relatório demonstrando as verificações realizadas sob a ótica da gestão de acessos, proteção de ambientes, segurança física e lógica e continuidade do negócio.





**CoopCREDER** Cooperativa de Economia e Crédito Mútuo  
dos Colaboradores da Coopeder Ltda.


## TERMO DE CIÊNCIA

O Conselho de Administração da Cooperativa de Economia e Crédito Mútuo dos Colaboradores da Coopeder Ltda, abaixo assinados, reforçam o compromisso com a adoção das boas práticas de governança corporativa e de gestão, proporcionais à relevância dos serviços oferecidos aos associados da CoopCREDER, tendo em vista o atendimento da Resolução CMN N° 4.893/2021 que trata da Política de Segurança Cibernética e os requisitos necessários para contratação de serviços de processamento e armazenamento de dados em nuvem. Assim sendo, o Conselho de Administração tomou ciência do conteúdo da Política de Segurança Cibernética e, após leitura ele foi aprovado em reunião realizada em 30 de maio de 2023, sendo devidamente assinado.

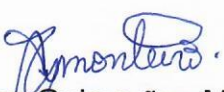
Belo Horizonte - MG, 30 de maio de 2023.

  
Zacarias Monteiro dos Santos  
Diretor Presidente

  
Fátima Eugênia de Araújo Camargo  
Conselheira

  
Egler José da Costa  
Conselheiro

Maria José de Oliveira Kurschus  
Conselheira

  
Telma Guimarães Monteiro  
Conselheira