**MODELO Nº 007/2020**

***(Observação:*** *Este modelo apresenta sugestões que devem ser avaliadas e adaptadas de acordo com as particularidades da Cooperativa.)*

**Política de Segurança Cibernética**

# **Apresentação**

Esta Política de Segurança Cibernética tem como objetivo assegurar a proteção dos ativos de informação da ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa)*** contra ameaças internas ou externas e definir processos e controles que visam reduzir a exposição a perdas ou danos decorrentes de falhas de segurança cibernética.

Esta política estabelece também diretrizes para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem conforme requisitos publicados pela Resolução nº 4.658/18 publicada pelo Conselho Monetário Nacional (CMN).

# **Aplicabilidade**

Aplica-se ao ***\_\_\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa***), colaboradores, estagiários e prestadores de serviços (descrever conforme estrutura da cooperativa).

# **Conceitos**

1. 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;
2. 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;
3. 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;
4. risco cibernético: ameaça à confidencialidade, integridade e disponibilidade das informações.

# **Regulamentação**

Para esta política estão associadas a Resolução 4.658/2018 publicado pelo Conselho Monetário Nacional (CMN) e a Política de Segurança da Informação da Cooperativa.

# **Responsabilidades:**

Todo componente da estrutura organizacional da cooperativa, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações e deve cumprir as determinações desta política, normas e padrões de segurança cibernética.

# **ÓRGÃO DE ADMINISTRAÇÃO *(descrever o órgão de administração da cooperativa responsável pelas atribuições)***

# São responsabilidades da ***\_\_\_\_\_\_\_\_(descrever o órgão de administração da cooperativa responsável pelas atribuições):***

1. aprovar esta política de segurança cibernética, o plano de ação e de respostas de incidentes;
2. prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética;
3. manter comprometimento e apoio à aderência a política de segurança cibernética de acordo com os objetivos e estratégias de negócio estabelecidas para organização;
4. fornecer à área de segurança da informação e cibernética claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário;
5. fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança cibernética.

# **DIRETOR RESPONSÁVEL PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA**

São responsabilidades do diretor responsável pela política de segurança cibernética:

1. propor melhorias nas diretrizes da política de segurança cibernética e no plano de ação;
2. acompanhar se as diretrizes da política estão sendo executadas;
3. executar o plano de ação e de respostas de incidentes.

# **GERÊNCIA / SUPERVISÃO / COORDENAÇÃO *(descrever áreas e/ou cargos conforme estrutura da cooperativa)***

São responsabilidades dos gestores

1. garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança de cibernética;
2. avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
3. 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;
4. autorizar acessos de seus colaboradores apenas quando forem realmente necessários.

# **ÁREA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA**

São responsabilidades da Área de Segurança da Informação e Cibernética:

1. desenvolver e estabelecer programas de conscientização e divulgação da política de segurança cibernética;
2. conduzir o processo de gestão de riscos de segurança cibernética;
3. conduzir a gestão de incidentes de segurança cibernética, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

conduzir a definição controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas;

1. propor projetos e iniciativas para melhoria do nível de segurança das informações da cooperativa.

# **SÃO RESPONSABILIDADES DOS COLABORADORES**

São responsabilidades dos Colaboradores:

1. notificar a área segurança da informação e cibernética os incidentes de segurança que venha a tomar conhecimento e as violações desta política de segurança cibernética;
2. utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de segurança cibernética.

# **PRINCÍPIOS E PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA**

A implementação desta política considera o porte, perfil de risco e modelo de negócios da cooperativa, considerando suas operações, produtos, serviços e processos atuais e ainda para atender a esta política baseia -se nos seguintes princípios:

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

# **SERVIÇOS DE COMPUTAÇÃO EM NUVEM**

Em atendimento a Resolução nº. 4.658/18 os serviços de computação em nuvem da abrange:

1. empregar de recursos computacionais dos prestadores de serviços em casos de implantação, execução de aplicativos adquiridos ou desenvolvidos pela cooperativa;
2. processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos que permitam a cooperativa implantar e executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos;
3. usar de recursos computacionais do próprio prestador de serviços para execução por meio de internet dos aplicativos implantados ou desenvolvidos.

Na gestão dos serviços contratados devem ser avaliados a confiabilidade, integridade, disponibilidade , segurança e sigilo das informações, os recursos utilizados, bem como o cumprimento da legislação vigente.

# **plano de ação**

Na implementação desta política a ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa)*** está implementando o plano de ação e respostas a incidentes compreendendo procedimentos, controles e tecnologias para prevenção e respostas a incidentes.

O plano de ação e resposta a incidentes deve ser aprovado pelo ***\_\_\_\_\_\_\_\_(órgão de administração da cooperativa)*** e revisado anualmente.

# **RELATÓRIO DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES**

A cooperativa deverá emitir anualmente o relatório de implementação de plano de ação e respostas a incidentes.

Os referidos relatórios devem ser aprovados diretor responsável pela segurança cibernética.

O relatório deverá ser emitido até 31 de dezembro e conter, no mínimo, as seguintes informações:

1. resumo dos resultados alcançados na implementação de rotinas, procedimentos e tecnologias utilizados na prevenção e na resposta a incidentes;
2. a efetividade alcançada na implementação da desta política;
3. as ocorrências de incidentes relevantes ocorrido no período relacionado referente ao ambiente cibernético;
4. resultados de testes de continuidade de negócios;

# **CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM**

A computação em nuvem é uma forma de contratação de serviços de terceiros, e esses prestadores de serviços de processamento e armazenamento de dados 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:

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

A ***\_\_\_\_\_\_\_\_(denominação da 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 ***\_\_\_\_\_\_\_(denominação da 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.

# **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 – BCB nas seguintes informações;

1. contratos e aos acordos firmados para a prestação de serviços;
2. documentação e às informações referentes aos serviços prestados;
3. dados armazenados e às informações sobre seus processamentos;
4. cópias de segurança dos dados e das informações;
5. códigos de acesso aos dados e às informações;
6. adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e
7. 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:

1. 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
2. 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:

b.1) 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;

b.2 a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

# **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:

1. manter relatório de inventários de *hardware* e *software*;
2. verificar com frequência se há na cooperativa computadores não autorizados ou *software* não licenciado;
3. manter os sistemas operacionais e *software* atualizados;
4. realizar frequentemente testes de invasão externa e *pishing*;
5. fazer análises de vulnerabilidade na estrutura tecnológica da cooperativa frequentemente ou em situações que houver mudança significativas;
6. fazer teste do plano de resposta a incidentes com simulação de cenários.

# **TRATAMENTO DE INCIDENTES**

Os incidentes são interrupções de sistema tecnológico não planejados que afetam os negócios das cooperativas e podem acontecer nas seguintes situações;

1. queda de energia;
2. falha de um elemento de conexão ou servidor fora do ar;
3. ausência de conexão com a internet;
4. terrorismo;
5. ataques de DDOS;
6. 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:

1. avaliar o impacto do incidente na cooperativa;
2. redirecionar as linhas de telefones para os celulares, instruir o provedor de telefonia a desviar linhas de dados, entre outros;
3. 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;
4. comunicar tempestivamente ao Banco Central do Brasil (BCB) 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, os diretores e equipe de contingência da cooperativa devem ser informados imediatamente e na retomada dos processos deverão ser definidos ações que incluem a análise procedimentos para que a cooperativa possa operar normalmente, bem como reconstrução de eventuais sistemas e mudanças e medidas de prevenção.

# **Declaração de Responsabilidade**

Os colaboradores e prestadores de serviços diretamente contratados pela ***\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa)*** devem aderir formalmente a um termo comprometendo-se a agir de acordo com a Política de Segurança Cibernética.

Os contratos firmados com a ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa)*** possuir cláusula que assegure a confidencialidade das informações protegidas por sigilo e pela legislação e regulamentação vigentes.

# **DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA**

Devem ficar à disposição do Banco Central do Brasil (BCB):

1. a presente Política;
2. a ata do ***\_\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa que aprovou a política, podendo ser o conselho de administração, diretoria executiva ou diretoria )*** com a aprovação da política;
3. documento relativo ao plano de ação e de resposta a incidentes;
4. relatório anual e a documentação sobre os procedimentos;
5. documentação que trata no caso de serviços prestados no exterior;
6. os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
7. os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade da Política se Segurança Cibernética;

As informações acima devem ficar à disposição do BCB pelo prazo de 05 (cinco) anos.

# **Treinamento**

A ***\_\_\_\_\_\_\_\_\_\_\_\_(denominação da cooperativa)*** deve estabelecer um programa de conscientização em Segurança Cibernética à garantia dos objetivos e diretrizes definidos nesta Política a fim de apresentar às necessidades e responsabilidades específicas de cada colaboradores.

# **revisão**

Esta Política será revisada anualmente pela \_\_\_\_\_\_\_\_\_\_\_\_(***descrever a área responsável)*** e sua aprovação caberá **\_\_\_\_\_\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa).**

# **considerações finais**

A (O) ***\_\_\_\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa)*** compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta Política.

Os indícios ou irregularidades devem ser comunicadas a área de segurança da informação e cibernética.

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e prestadores de serviços com abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

Esta política é aprovada pelo ***\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa***) e comunicada a todos os colaboradores e partes interessadas que sejam relevantes para o cumprimento necessário.

Esta política foi aprovada na reunião do ***\_\_\_\_\_\_\_\_\_(órgão de administração da cooperativa***) realizada em \_\_\_\_\_/\_\_\_\_/\_\_\_\_.