ÍNDICE

1. OBJETIVO....2
2. RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS....2
3. ÁREA GESTORA DA POLÍTICA DE SEGURANÇA CIBERNÉTICA....3
4. DIRETRIZES....3
5. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES....4
5.1. IMPLEMENTAÇÃO DA POLÍTICA....4
5.2. RELATÓRIO SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES....5
6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM....5
6.1 EXIGÊNCIAS PARA A CONTRATAÇÃO DE SERVIÇOS....5
6.2 AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS....6
6.3. COMUNICAÇÕES AO BANCO CENTRAL....7
6.4. DOS CONTRATOS....8
7. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO....9
7.1. MITIGAÇÃO DOS RISCOS....9
7.2. AÇÕES DE PREVENÇÃO....10
7.3. TRATAMENTO DE INCIDENTES....10
7.4. MONITORAMENTO E TESTES....12
7.5. PLANO DE CONTINUIDADE DE NEGÓCIOS....12
7.6. CONSCIENTIZAÇÃO E TREINAMENTO....13
7.7. PRIVACIDADE E PROTEÇÃO DE DADOS....13
7.8 COMPARTILHAMENTO DE INFORMAÇÕES....13
8. DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL....13
9. REGULAMENTAÇÃO ASSOCIADA....14
10. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA....14

1. OBJETIVO

Este normativo estabelece a Política de Segurança Cibernética da COOPERFEMSA, bem como os requisitos para a Contratação, Avaliação e Gestão de serviços de processamento e armazenamento de dados e de computação em nuvem visando total observância e adequação ao exigido na Resolução nº 4.893/21 do Banco Central do Brasil.

O principal objetivo desta Política é assegurar a proteção dos ativos de informação da Cooperativa 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 de nossos negócios.

2. RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, colaboradores, competidores etc.) como por exemplo:

- Ganhos financeiros através de roubo, manipulação ou adulteração de informações;
- Obter vantagens competitivas e informações confidenciais de Cooperados ou Instituições concorrentes.
- Fraudar, sabotar ou expor a Instituição invadida por motivos de vingança, idéias políticas ou sociais.
- Praticar o terror e disseminar pânico e caos.
- Enfrentar desafios e/ou ter adoração por hackers famosos.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

Tantos as instituições grandes como as menores podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados sendo também essa necessidade um dos motivos da implementação desta Política.

Entre esses ativos cibernéticos estão:

- Softwares, como um programa de computador;
- Conectividades como acesso a internet, Banco Central, Receita Federal, etc.;
- Informações sigilosas de cooperados;
- Componentes físicos, como servidores, estações de trabalho, notebooks, etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central através da Resolução nº 4.893/21 já mencionada, têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

3. ÁREA GESTORA DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Responsável: Diretor responsável pela Política de Segurança Cibernética

Atribuições:
– Responsável pela Política de Segurança Cibernética
– Responsável pela execução do Plano de Ação e de Resposta a Incidentes

O Diretor responsável pela Política de Segurança Cibernética pode desempenhar outras funções na Cooperativa desde que não haja conflitos de interesses.

4. DIRETRIZES

A Política de Segurança Cibernética, que está sendo implementada na COOPERFEMSA baseia-se nos seguintes princípios:

- Assegurar a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) observadas as regras de sigilo e confidencialidade vigentes.

- Assegurar a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);

- Assegurar a disponibilidade dos dados e sistemas de informação utilizados na Cooperativa (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário).

A implementação desta Política considera as seguintes compatibilidades da Cooperativa:

a) O porte, perfil de risco e o modelo de negócios;

b) A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais.

c) A sensibilidade dos dados e das informações sob responsabilidade da instituição.

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

Caberá a todos os colaboradores conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

Conforme a Resolução nº 4.893/21, os serviços de computação em nuvem abrangem a disponibilidade da COOPERFEMSA, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

a) Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à COOPERFEMSA implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos.

b) Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela COOPERFEMSA utilizando recursos computacionais de seus prestadores de serviços.

c) Execução por meio de Internet dos aplicativos implantados ou desenvolvidos por prestadores de serviços da COOPERFEMSA, com utilização de recursos computacionais do próprio prestador de serviços contratado pela Cooperativa.

A COOPERFEMSA é responsável pela gestão dos serviços contratados incluindo as seguintes atividades:

a) Análises de informações e de recursos adequados ao monitoramento dos serviços.

b) Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto aos prestadores de serviços.

c) Cumprimento da legislação e da regulamentação vigente.

5. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES

5.1. IMPLEMENTAÇÃO DA POLÍTICA

Visando a implementação das práticas da Política de Segurança Cibernética, a COOPERFEMSA está implementando um Plano de Ação e de resposta a incidentes abrangendo o seguinte:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética.
- Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes.
- Área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Plano de Ação e de Resposta a Incidentes será aprovado pelo Diretor responsável pela Política de Cibernética e será revisado no mínimo anualmente.

5.2. RELATÓRIO SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Será emitido anualmente, com data base de 31 de dezembro, relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes.

Esse Relatório deve contemplar, no mínimo, as seguintes informações:

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

O relatório deve ser elaborado até 31 de março do ano seguinte ao da data base devendo ser aprovado pelo Diretor responsável pela Segurança Cibernética.

6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Os prestadores de serviços e parceiros de serviços de processamento de dados e armazenamento em nuvem podem representar uma fonte significativa de riscos de cibersegurança.

A computação em nuvem é considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações, envolve determinados riscos que são levados em conta pela Cooperativa, demandando assim cuidados proporcionais a esta identificação de ameaças.

6.1 EXIGÊNCIAS PARA A CONTRATAÇÃO DE SERVIÇOS

A COOPERFEMSA ao realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as seguintes exigências:

a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo:

- Se mantém Política de Segurança da Informação;
- Se possui Plano de Continuidade Operacional;
- Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças);
- Se mantém Gestão de Incidentes.

b) Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:

- Cumprimento da legislação e da regulamentação em vigor;
- Permissão de acesso da COOPERFEMSA aos dados e as informações a serem processadas ou armazenadas pelo prestador de serviços;
- Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviços;
- Aderência a certificações que a COOPERFEMSA possa exigir para a prestação do serviço a ser contratado;
- Acesso da COOPERFEMSA aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
- Provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- Identificação e segregação dos dados dos clientes COOPERFEMSA por meio de controles físicos ou lógicos.

Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados da COOPERFEMSA.

6.2 AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

A COOPERFEMSA deve proceder a uma avaliação da relevância dos serviços prestados por empresas com possibilidades de serem contratadas considerando o seguinte:

- Criticidade dos serviços a serem prestados;
- Sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;
- Verificação quanto a adoção, por parte do prestador de serviços, quanto aos controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet.

6.3. COMUNICAÇÕES AO BANCO CENTRAL

A COOPERFEMSA deverá informar previamente ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada 10 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 Banco Central no mínimo 10 dias após da alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela COOPERFEMSA, deve observar os seguintes requisitos:

a) A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

b) Assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

c) Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

d) Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anteriores, a COOPERFEMSA deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A COOPERFEMSA deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações.

6.4. DOS CONTRATOS

Os contratos firmados entre a COOPERFEMSA e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) A indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

b) A adoção de medidas de segurança para a transmissão e armazenamento dos dados;

c) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos cooperados;

d) A obrigatoriedade, em caso de extinção do contrato, de:

- Transferência dos dados ao novo prestador de serviços ou à COOPERFEMSA;
- Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

e) O acesso da COOPERFEMSA a:

- Informações fornecidas pela empresa contratada visando verificar o cumprimento previstos nos itens a), b) e c) acima;
- Informações relativas às Certificações exigidas pela Cooperativa e aos relatórios de auditoria especializada contratada pelo prestador de serviços;
- Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f) A obrigação da empresa contratada notificar à COOPERFEMSA sobre a subcontratação de serviços relevantes para a Cooperativa.

g) A permissão de acesso do Banco Central do Brasil às seguintes informações:

- contratos e acordos firmados para a prestação de serviços;
- documentação e informações referentes aos serviços prestados;
- os dados armazenados;
- as informações sobre processamento;
- as cópias de segurança dos dados e das informações;
- códigos de acesso aos dados e as informações.

h) A adoção de medidas pela COOPERFEMSA em decorrência de determinação do Banco Central do Brasil.

i) A obrigatoriedade da empresa contratada manter à COOPERFEMSA permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor.

j) O contrato deve também prever, para o caso de decretação de regime de resolução da Cooperativa pelo Banco Central:

- A obrigação da empresa contratada para a prestação de serviços conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada.
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:
  - A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
  - A notificação prévia deve ocorrer também na situação em que a interrupção for motivada por inadimplência da Cooperativa.

7. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

7.1. MITIGAÇÃO DOS RISCOS

Está sendo estabelecido um conjunto de medidas buscando mitigar os riscos de forma a impedir previamente a ocorrência de um ataque cibernético.

A Cooperativa oferece aos colaboradores uma completa estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (computador, notebook, acesso à internet, E-mail, etc.).

Equipamentos e computadores disponibilizados aos colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Cooperativa.

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

As mensagens enviadas ou recebidas através do correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da Cooperativa poderão ser monitoradas.

As senhas para acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.) compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

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

7.2. AÇÕES DE PREVENÇÃO

Devem ser criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da Cooperativa através das seguintes ações:

- Manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição. Por exemplo, computadores não autorizados ou software não licenciado;
- Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas;
- Monitorar rotinas de backup, executando testes regulares de restauração dos dados;
- Realizar, periodicamente testes de invasão externa e phishing;
- Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura;
- Periodicamente testar o plano de resposta a incidentes, simulando os cenários.

7.3. TRATAMENTO DE INCIDENTES

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

- queda de energia elétrica;
- falha de um elemento de conexão;
- servidor fora do ar;
- ausência de conexão com internet;
- sabotagem / terrorismo;
- Indisponibilidade de acesso a cooperativa;
- Ataques DDOS.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato para que o mesmo seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

AVALIAÇÃO INICIAL

Avaliar o incidente em conjunto com o Conselho de Administração para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas

Analisar motivos e consequências imediatas, bem como a gravidade da situação.

INCIDENTE CARACTERIZADO

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

- Iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros;
- O Diretor responsável pela Política de Segurança Cibernética estará avaliando o impacto do incidente nos diversos riscos envolvidos;
- Conforme a relevância (sabotagem, terrorismo, etc.) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências;
- Conforme a relevância do incidente comunicar os cooperados que por ventura tenham sido afetados;
- Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela COOPERFEMSA.

RECUPERAÇÃO

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros-chave notificados.

Quaisquer dados faltando ou corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados ao Conselho de Administração.

RETOMADA

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

7.4. MONITORAMENTO E TESTES

O ambiente de TI da Cooperativa deve ser supervisionado e monitorado com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

É possível a ocorrência de algum risco de segurança cibernética através de uma das seguintes situações descritas:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas;
- Comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”);
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com condições internamente estabelecidas;
- Vazamento de informações durante tráfego de dados não criptografados.

Semestralmente a Cooperativa deve providenciar a execução de testes de cibersegurança através da verificação dos seguintes itens:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da Cooperativa;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Cooperativa;
- Vulnerabilidades que possam causar incidentes (vírus, trojans, furtos, acessos indevidos, etc.).

7.5. *PLANO DE CONTINUIDADE DE NEGÓCIOS*

A COOPERFEMSA estabelece diretrizes para o Plano de Continuidade de Negócios (PCN), visando contribuir para a resiliência e a sustentabilidade dos negócios antes, durante e depois de situações de crise através do planejamento, para uso em situações de crise previamente definidas e avaliadas pela cooperativa.

Diretrizes detalhadas estão documentadas em documento específico de Plano de Continuidade de Negócios.

7.6. *CONSCIENTIZAÇÃO E TREINAMENTO*

Deve ser mantido um programa de capacitação e avaliação de pessoal no que diz respeito à conscientização e disseminação do assunto Segurança da Informação e cibernética. Tal programa se aplica a todos os colaboradores e prestadores de serviço e ficará sob a responsabilidade da Área de Controles Internos. Tal programa pode ser composto por treinamentos, palestras, integrações de novos colaboradores, a fim de assegurar que estes possuam formação para desempenhar as suas funções e responsabilidades de forma coerente com as políticas e procedimentos de segurança pertinentes para reduzir o erro humano, o roubo, a fraude, a utilização indevida ou a perda e de forma a abordar os riscos relacionados com a segurança da informação.

7.7. *PRIVACIDADE E PROTEÇÃO DE DADOS*

As regras e diretrizes de Privacidade e Proteção de Dados, estão estabelecidas em política específica de Privacidade e Proteção de Dados Pessoais, em conformidade com a Lei Geral de Proteção de Dados – LGPD.

7.8 COMPARTILHAMENTO DE INFORMAÇÕES

A COOPERFEMSA em conjunto com outras cooperativas criou um grupo de trabalho para avaliar alternativas de compartilhamento de informações sobre incidentes relevantes com instituições congêneres, incluindo no mínimo registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, abrangendo:

a) Compartilhamento de Informações entre as cooperativas;
b) Compartilhamento das Informações com o Banco Central.

8. DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- Política de Segurança Cibernética;

- Ata de Reunião da Diretoria Executiva da Cooperativa implementado a Política de Segurança Cibernética;
- Documento relativo ao Plano de Ação e de resposta a incidentes relativos à implementação da Política de Segurança Cibernética;
- Relatório anual sobre a implementação do Plano de ação e de resposta a incidente;
- Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra;
- Contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem.
- 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.

9. REGULAMENTAÇÃO ASSOCIADA

Resolução Bacen nº 4.893, de 26 de fevereiro de 2021.

10. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

O conteúdo desta Política de Segurança Cibernética política aplica-se a todos os colaboradores e prestadores de serviços relevantes do COOPERFEMSA, no âmbito de suas atividades, atribuições e responsabilidades.

Está aprovada pela Diretoria Executiva o qual está comprometida com a melhoria contínua do disposto neste normativo.

Está sendo publicada e comunicada para todos os colaboradores, empresas contratadas de serviços de cibernética, cooperados e partes externas relevantes, para o necessário cumprimento.

Um resumo da Política de Segurança Cibernética estará sendo divulgado ao público através do site da Cooperativa.

É obrigação de todo colaborador conhecer e praticar às disposições desta política e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas.

Será implementado um Programa de Capacitação e de Avaliação periódica de pessoal sobre as diretrizes desta política.

Esta política, juntamente com o plano de ação e respostas a incidentes será revisada anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia.