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 4.658/18 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 4.658/18 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. DIRETRIZES

A Política de Segurança Cibernética, 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 4.658/18, 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.

4 IMPLEMENTAÇÃO DA POLÍTICA

Visando a implementação das práticas da Política de Segurança Cibernética, a COOPERFEMSA implementa 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 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. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

6.1 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 Politica 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.

6.2 AÇÕES DE PREVENÇÃO

São 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.

6.3 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 aos 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.

6.4 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 ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLITICA

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 pelo Conselho de Administração o qual está comprometido 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. Além de ser divulgada 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.