POLÍTICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

1 – INTRODUÇÃO

A Resolução nº 4.658/18 do Conselho Monetário Nacional estabelece as exigências para as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil quanto aos seus ambientes de tecnologia contra os ataques cibernéticos.

Portanto, se torna necessário dispor de uma política de segurança e sobre as premissas de contratação de serviços de computação em nuvem e de processamento e armazenamento de dados. A Resolução também obriga o desenvolvimento de cenários de incidentes possíveis e como eles seriam solucionados pela Cooperativa.

A segurança cibernética é um conjunto de práticas que protege as informações armazenadas nos computadores e dispositivos móveis, transmitidas através das redes de comunicação, como a internet, telefones celulares e arquivos em nuvem. Todos os computadores conectados à internet estão vulneráveis a ataques, entretanto, há maneiras de evitá-los.

As instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil deverão manter a política de segurança cibernética, 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.

A Cooperativa, com o objetivo de prevenir, detectar e reduzir os impactos gerados pelos incidentes relacionados ao ambiente cibernético e em conformidade com as melhores práticas de mercado e da legislação aplicada, implantou a **Política de Segurança Cibernética**.

Aprovada pela Diretoria, esta política foi elaborada para tratar e prevenir incidentes de segurança cibernética, reforçando o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética da **COOPERMSD**.

Estabelece também, os requisitos para a contratação, avaliação e gestão de serviços de processamento e armazenamento de dados e de computação em nuvem.

A política está compatível com:

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

b) A natureza das operações e a complexidade dos produtos, serviços, atividades e processos da Cooperativa;
c) A sensibilidade dos dados e informações sob sua responsabilidade.

Nota: A Cooperativa atende somente os funcionários da empresa com prazo indeterminado e está enquadrada no segmento de **capital e empréstimo**, categoria **S5**, onde o nível de risco é considerado baixo, de estrutura simplificada e consignação em folha de pagamento.

2 – OBJETIVO

A Política de Segurança Cibernética da Cooperativa visa:

- Definir diretrizes para a segurança do espaço cibernético;
- Proteger as informações sob responsabilidade da Cooperativa preservando sua confidencialidade, integridade, disponibilidade e autenticidade;
- Prevenir eventuais interrupções, totais ou parciais, e no caso de sua ocorrência, reduzir os impactos dela resultantes;
- Tratar e prevenir incidentes de segurança cibernética;
- Formar e qualificar os envolvidos necessários à área de segurança cibernética;
- Promover o intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética;
- Definir os requisitos para a contratação, avaliação e gestão de serviços de processamento e armazenamento de dados e de computação em nuvem;
- Viabilizar a confiança nos relacionamentos entre a Cooperativa e seus colaboradores.

3 – ABRANGÊNCIA

Todos os usuários que compõem a estrutura organizacional da Cooperativa (dirigentes, conselheiros fiscais e funcionários) e demais pessoas com acesso autorizado às informações da Instituição, incluindo associados, colaboradores e empresas prestadoras de serviço relevantes no âmbito de suas atividades, atribuições e responsabilidades.

4 – RESPONSABILIDADE

❖ A Diretoria é responsável pelo gerenciamento da segurança cibernética na Cooperativa:

a) Revisar e aprovar anualmente a política e estratégias de gerenciamento de segurança cibernética;

b) Assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de segurança cibernética;

c) Promover a disseminação da cultura de gerenciamento de segurança cibernética;

d) Definir o diretor responsável pela gestão de segurança cibernética.

❖ Conforme determina a Resolução nº 4.658/18 do Conselho Monetário Nacional, a Cooperativa indicou o diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes conforme cadastrado no Unicad.

O diretor responsável pela segurança cibernética tem como atribuições:

a) Responsável pela Política de Segurança Cibernética;

b) Responsável pela execução do Plano de Ação e de Resposta a Incidentes;

c) Supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de segurança cibernética, incluindo seu aperfeiçoamento;

d) Subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética;

e) Responsabilizar-se pela capacitação adequada dos funcionários que compõem a estrutura de gerenciamento de segurança cibernética, acerca das políticas, dos planos e dos controles.

❖ Os funcionários devem:

a) Observar e executar os procedimentos descritos na política, planos e controles relativos ao tema;

b) Sugerir aperfeiçoamento da política, planos, controles e procedimentos relacionados à segurança cibernética;

c) Reportar ao diretor responsável, informações relevantes referentes à segurança cibernética.

❖ Em relação à estrutura contratada da gestão de segurança cibernética da Cooperativa:

a) Providenciar o relacionamento com órgãos de supervisão internos e externos;

b) Prestar apoio a Cooperativa contratante, relativo à gestão de segurança cibernética;

c) Informar à Cooperativa contratante sobre os incidentes cibernéticos relevantes;

d) Reportar a Diretoria da Cooperativa as informações relativas à gestão centralizada de segurança cibernética;

e) Compartilhar informações sobre incidentes cibernéticos relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

5 – DIRETRIZES

A segurança da informação da Cooperativa estabelece os principais controles, denominados diretrizes, conforme mencionada em nossa política de segurança da informação (alinhadas a esta política), onde destacamos:

a) A informação deve ser utilizada de forma transparente e para a finalidade para a qual foi coletada;

b) As informações confidenciais da Cooperativa, dos seus associados, de todos os envolvidos, devem ser tratadas de forma ética, sigilosa, de acordo com as leis vigentes e normas internas, evitando-se o mau uso e exposição indevida;

c) A Cooperativa conforme o porte, o perfil de risco, o modelo de negócio da instituição; a natureza das operações, a complexidade dos produtos, serviços, atividades, processos da instituição; a sensibilidade dos dados e das informações sob responsabilidade da instituição; observa em todo processo, durante o seu ciclo de vida, garantir a segregação de funções, por meio da participação de mais de um colaborador, para que a atividade não seja executada e controlada por uma única pessoa.

A Cooperativa transita somente dados pessoais (significa quaisquer informações relacionadas a pessoa natural identificada como seu nome, sobrenome, idade, endereço, e-mail, RG, CPF, entre outros).

A coleta de dados pessoais sensíveis dependendo de uma prestação de serviços de saúde, poderão ser coletadas informações obtidas a partir de análises ou exame de uma parte do corpo, dados genéticos, biométricos, doenças, dados sobre deficiências, risco de doença, tratamentos e prontuários;

d) O acesso às informações e recursos só deve ser feito se devidamente autorizado;

e) A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

f) A concessão de acessos deve obedecer aos critérios, no qual os usuários têm acesso somente aos recursos e informações imprescindíveis para o pleno desempenho de suas atividades;

g) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

h) Os riscos às informações da Cooperativa devem ser reportados ao diretor responsável;

i) As responsabilidades quanto à segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem entender e assegurar estas diretrizes.

Os funcionários e prestadores de serviços relevantes deverão conhecer e adotar as disposições desta política e 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.

Poderão ser monitorados e gravados, os ambientes, sistemas, computadores, redes da Cooperativa conforme previsto nas leis brasileiras.

Conforme a Resolução nº 4.658/18, os serviços de computação em nuvem abrangem a disponibilidade da Cooperativa, 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 a Cooperativa implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos;

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

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

A Cooperativa 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 a prestadores de serviços;
c) Cumprimento da legislação e da regulamentação vigente.

6 – PROTEÇÃO DA INFORMAÇÃO

A informação deve receber proteção adequada em observância aos princípios e diretrizes de segurança da informação da Cooperativa em todo seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

7 – PROCEDIMENTOS E CONTROLES

Para reduzir a vulnerabilidade da Cooperativa a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, a **COOPERMSD** deverá adotar procedimentos e controles, conforme o porte e perfil de risco da entidade:
a) Regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade da Cooperativa;
b) Duplo fator de autenticação nos ambientes em que o recurso está disponível;

c) Recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados mantidos pela Cooperativa;

d) Solução de prevenção e detecção de intrusão, solução de proteção de dispositivos, procedimentos de **hardening**, monitoramento de tráfego na rede, monitoramento de atividades em bancos de dados, monitoramento de atividade de usuários privilegiados;

e) Testes de invasão realizados por empresas contratadas e processo de gestão de vulnerabilidades de ativos de TI;

f) Solução de proteção contra ameaças avançadas em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus de borda;

g) Gerenciador de eventos e incidentes em segurança que mantém registro dos eventos do ambiente, permitindo a rastreabilidade de vários tipos de ocorrências;

h) Segmentação de rede, com isolamento de ambientes (como produção e homologação) e áreas;

i) Manutenção de cópias de segurança dos dados e das informações.

Os procedimentos e controles serão aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

Estes procedimentos e controles aplicados tem o apoio e suporte da empresa patrocinadora, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis e conta também, com os serviços contratados das empresas terceirizadas – Fácil Informática, responsável pelo sistema operacional da Cooperativa e da empresa - SaveMais Tecnologia Ltda, serviços de hospedagem do site, manutenção e suporte técnico de informática.

Apresentamos as principais orientações para manter o computador seguro conforme a nossa política de segurança da informação:

- Instalar um bom programa de antivírus (atualização constante) e, pelo menos uma vez por semana, realizar uma verificação completa do computador;
- Manter o sistema operacional do computador e seus programas sempre atualizados para protegê-los contra as falhas de segurança;
- Instalar programas legítimos, de fonte confiáveis, nunca “piratas”;
- Não abrir e-mails e arquivos enviados de fontes desconhecidas;

- Estabelecer senhas para os compartilhamentos de recursos e permissões de acesso adequadas;
- Atentar aos endereços acessados no seu navegador;
- Procurar por sites reconhecidamente seguros quando efetuar compras pela internet;
- Sempre procurar pelos sinais de segurança ao utilizar internet banking;
- Trocar as senhas com frequência, ela é pessoal e intransferível, e, criada de acordo com as funções permitidas para o exercício das suas atividades;
- Procurar sempre acessar redes seguras;
- Realizar e monitorar backup periodicamente de todos os arquivos e sistemas;
- Manter os inventários atualizados de hardware e software atualizados, de forma a detectar qualquer computador ou notebook não autorizados ou software não licenciado;
- Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em sua estrutura;
- Ao detectar algum erro é importante que seja rastreado, através das tecnologias disponíveis, todo o caminho do processo, para, assim, corrigir o ponto onde o erro aconteceu ou iniciou.

Os procedimentos buscam abranger no mínimo a autenticação, criptografia, prevenção, detecção e possíveis vazamentos de informação, a realização periódica de testes e varreduras para detecção de vulnerabilidade, bem como a proteção contra software maliciosos, e o estabelecimento de mecanismos de rastreabilidade.

Busca prover ainda, o controle de acesso, segmentação da rede, a manutenção de cópias de segurança dos dados e das informações e o desenvolvimento de sistemas seguros.

Nota 1: Orientamos que no caso de dúvida não execute nenhum procedimento sem conhecimento e procure orientação específica de pessoas habilitadas (Suporte da empresa patrocinadora, da Empresa contratada – SaveMais ou prestador de serviço do sistema operacional – Fácil) para sanar quaisquer dúvidas e executar os procedimentos com segurança.

Nota 2: A empresa patrocinadora garante e controla a parte da rede; os serviços de manutenção preventiva; suporte remoto; atualizações de segurança; configurações necessárias; antivírus; gestão e proteção no recebimento dos e-mails, bloqueando o SPAM, Malwares e links maliciosos (Exchange Online); entre outros procedimentos. Existe um controle de acesso ao e-mail, arquivos e computadores com usuário e senha.

É estabelecido plano de ação e de resposta a incidentes, revisado anualmente.

8 – PROCESSOS DE SEGURANÇA

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Cooperativa adota os seguintes processos:

a) **Gestão de Ativos da Informação**

Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas).

Os ativos da informação devem ser identificados de forma individual, inventariado e protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção.

O software gerenciador da **COOPERMSD** está devidamente formalizado por meio de contrato de uso e licença com a empresa Fácil Informática responsável pelo sistema operacional (CT-NUV-22014-2019).

A empresa periodicamente disponibiliza novas versões para sempre manter o sistema atualizado.

b) **Classificação da Informação**

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

A classificação está definida em 3 (três) níveis em ordem crescente:

✓ Públicas: são todas as informações publicadas para todos os empregados, diretores, associados, prestadores de serviços e público em geral, por meio de quadro de avisos ou mural, através da internet ou qualquer outra mídia;

✓ Internas: são informações disponíveis apenas para os empregados, diretores ou associados através de autorização. Essa informação é de responsabilidade da **COOPERMSD** e não poderá ser divulgada e nem disponibilizada para outros;

✓ Confidencial: são informações de acesso restrito mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis, como cofres, armários com chaves e diretório.

Nota: As informações de propriedade/custódia da Cooperativa, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

c) **Gestão de Acessos**

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Cooperativa.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passiveis de auditoria possam identificar individualmente o colaborador, para que seja responsabilizado por suas ações.

d) **Gestão de Riscos**

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos de informação da Cooperativa, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos setores apropriados, para decisão.

e) **Tratamento de Incidentes de Segurança da Informação e Cyber Security;**
Cyber Security/Cyber Segurança *é o termo que designa o conjunto de meios e tecnologias que visam proteger, de danos e intrusão ilícita, programas, computadores, redes e dados. Também conhecida como segurança do ciberespaço, a* ***cibersegurança*** *tem se tornado uma preocupação para muitas pessoas e nações.*

Os incidentes de Segurança da Informação e cibernéticos da Cooperativa devem ser reportados ao Diretor responsável/Diretoria.

f) **Segurança Física do Ambiente** (Acesso físico somente a pessoas autorizadas).

9 – GERENCIAMENTO DE INCIDENTES

O objetivo é assegurar que os eventos de segurança da informação sejam tratados de forma efetiva, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de informação da Cooperativa.

Os Procedimentos compreendem:

I – Recepção da denúncia/atividade suspeita: Serão aceitas denúncias e a Cooperativa colaborará com os órgãos legalmente competentes na investigação de atividades presumidamente ilícitas provenientes da rede da Cooperativa, onde serão investigados, iniciando o processo de tratamento de incidentes de segurança quando for observada atividade em desacordo com procedimentos éticos e padrões.

II – Medidas de controle: A contenção imediata do incidente se fará por meio de bloqueio de acesso do host envolvido à rede até o termino da investigação.

*“**host** é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes. Por essa abrangência, a palavra pode ser utilizada como designação para diversos casos que envolvam uma máquina e uma rede, desde computadores pessoais à roteadores”.*

III – Coleta, análise das informações e evidências: Serão coletadas informações e evidências sobre as atividades denunciadas através dos logs dos diversos sistemas e serviços disponíveis na rede da Cooperativa. Serão analisadas para investigar o host que gerou o incidente denunciado. A identificação do host compreenderá a determinação do seu endereço IP e endereço MAC da interface de rede, nome, switch, porta de acesso, usuário e todas outras informações possíveis.

*“**Endereço IP** significa endereço de protocolo de Internet, e cada dispositivo que está conectado a uma rede (como a Internet) possui um”.*
*“**MAC** é a sigla de Media Access Control, ou seja, o **Endereço MAC** nada mais é que o endereço de controle de acesso da sua placa de rede”.*

O tipo de atividade será determinado pelas informações evidenciadas em logs de serviços. As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

IV – Notificação: Será encaminhada notificação por escrito da atividade denunciada ou sob investigação (origem da atividade e sua comprovação) à direção da Cooperativa.
Como origem das atividades pode considerar:

- Atividade realizada pelo usuário;
- Atividade realizada por terceiro com autorização do usuário;

- Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

Como evidência da origem da atividade pode-se considerar:

- Logs de acesso local ou remoto na máquina;
- Logs de detecção de vírus, spyware, malware (software malicioso), etc...

*"**Spyware** é um software espião de computador, que tem o objetivo de observar e roubar informações pessoais do usuário que utiliza o PC em que o programa está instalado, retransmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário".*

- Outras informações que possam identificar claramente a origem da atividade.

A Diretoria notificada com auxílio do suporte de tecnologia das empresas contratadas, deverá responder a notificação por escrito, com a comprovação da origem da atividade e as medidas administrativas tomadas para evitar reincidências do usuário.

V – Medidas corretivas: A Diretoria avaliará a resposta e determinará as medidas corretivas no host identificado. Nos casos comprovados de invasão e de atividades maliciosa de usuário, o host permanecerá bloqueado até a implantação das medidas corretivas apresentadas.

Nota: O funcionário ao detectar um incidente deverá comunicar imediatamente, levando ao conhecimento do ocorrido ao Diretor Responsável/Diretoria.

A Diretoria e os envolvidos irão avaliar o incidente (os motivos, gravidade, consequências) para a tomada de decisão (providências necessárias e medidas corretivas).
Caracterizado o incidente, medidas imediatas devem ser tomadas, como: avaliação do impacto do incidente nos riscos envolvidos pelo diretor responsável; boletim de ocorrência se for o caso; comunicação aos associados caso tenham sido afetados; outros direcionados a redundância de TI, provedor de telefonia, e-mail, entre outros.

Comunicação tempestiva ao Banco Central do Brasil das situações de incidentes relevantes ocorridos e das interrupções dos serviços caracterizando crise pela Cooperativa.

A recuperação e a retomada ocorrem após o incidente ter sido sanado e o retorno operacional da Cooperativa voltando a sua normalidade onde o processo da ocorrência será comentado em relatório, bem como, as medidas de prevenção.

10 – PLANO DE AÇÃO/DE RESPOSTA A INCIDENTES/RELATÓRIO

O plano de ação e de resposta a incidentes abrangem:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética;

- Os controles, procedimentos, rotinas, e tecnologias a serem utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética;

- 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 segurança cibernética e será revisado no mínimo anualmente.
Será emitido anualmente, com data base de 31 de dezembro, relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes.

O Relatório deverá 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 (caso necessário) de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

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

11 – MONITORAMENTO E TESTES

As novas tecnologias e a integração entre elas trazem consigo novos pontos de ataque. Conforme a tecnologia evolui, a defesa da informação deve evoluir também. Muitos programas maliciosos invadem computadores por meses e meses, extraviando dados valiosos e úteis aos hackers. Todos os computadores conectados à internet estão vulneráveis. Há muitos tipos de ataques, sejam vírus, malwares, corrupção de rede, sobrecarga, etc.

A Cooperativa deverá monitorar o seu ambiente tecnológico, com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, para garantir o bom funcionamento e efetividade da segurança cibernética, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente de TI, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

A Cooperativa, sempre que necessário, deverá 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, comunicação falsa, link malicioso, ataque de hacker, etc.).

DESASTRE: Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo.

Procedimentos de gerenciamento:

a) TECNOLOGIA DA INFORMAÇÃO: O tempo é de até uma hora para que as atividades operacionais possam suportar a indisponibilidade de processos com os seguintes procedimentos:

✓ Suporte a retomada das operações;

✓ Preparar o ambiente de infraestrutura e sistemas para que todos possam dar continuidade na localidade backup;

b) SISTEMAS E INTERNET: O tempo é de até 6 (seis) horas, compreendendo o seguinte procedimento:

✓ Entrar em contato com a empresa Fácil Informática para comunicar o evento ocorrido;

✓ Identificar com o prestador de serviço o prazo para o restabelecimento do sistema;

c) HARDWARE E SOFTWARE: O tempo é de até 8 (oito) horas. Os procedimentos:

✓ Entrar em contato com o suporte de TI;

✓ Acompanhamento e suporte a retomada das operações.

O funcionário/colaborador da Cooperativa, ao constatar qualquer anormalidade que paralise quaisquer dos processos, deverá comunicar o fato ao seu superior imediato que comunicará ao Líder de Contingência.

O meio de comunicação a ser utilizado pelos colaboradores da **COOPERMSD** para solicitar orientação e informar alguma situação que demande o acionamento do Plano é:

Nome	Cargo / Função	Telefone	Responsável
Janete Aparecida Rogante janete_rogante@merck.com	Coordenadora Administrativa	(11) 5189-7936	Líder
Vanda Ferreira dos Santos Silva Vanda_santos@merck.com	Contadora	(11) 5189-7964	Suplente de Líder
Regiane Aparecida dos Santos regiane_dossantos@merck.com	Assistente Administrativo	(11) 5189-7754	Participante

Na ocorrência de eventos que paralise algum processo de continuidade de negócios da Cooperativa, o líder de Contingência irá avaliar a situação e comunicará ao Diretor responsável pelo plano.

O diretor responsável, irá avaliar as informações recebidas (grau de impacto/risco, horário crítico) responsabilizando pela declaração ou não à contingência.

Fluxo:

- Ocorrência de crise ou desastre;
- Funcionário comunica o diretor responsável e na sua ausência, a Diretoria;
- O líder da contingência avalia a situação que aciona o responsável pelo reparo;
- Se o reparo for concluído dentro do tempo previsto, não há necessidade de acionar o plano de contingência;
- O não reparo leva o líder de contingência a reunir os envolvidos no processo e declara a contingência – PCN (PCO e recuperação são acionados);
- O PCO fica em operação de contingência até o reparo ser concluído.

Em decorrência desses eventos, a Diretoria a fim de evitar futuros transtornos, visa evitar:

- Que os associados fiquem sem atendimento;
- Que a Cooperativa não consiga realizar os pagamentos e a liberação de empréstimos.

O funcionário/colaborador da Cooperativa deverá estar apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao líder do Plano de Continuidade de Negócios.

a) Em caso de danificação na infraestrutura, a estrutura de T.I. e Telecom, poderá ser restaurada em até um dia.

b) Se houver indisponibilidade de determinado serviço será acionada a contingência na empresa Fácil Informática.
Após constatação de falha no servidor local, a Cooperativa imediatamente, acionará o suporte de TI.
O suporte deverá providenciar uma nova estrutura de equipamentos de servidores nos casos de perdas de hardware através de uma nova instalação do ambiente Windows Server e realizará a restauração dos arquivos de rede através do backup.
Retorno à normalidade: até um dia após o incidente.

c) Em caso de instabilidade no Servidor Sistema, a Fácil Informática é acionada e o backup será disponibilizado conforme necessidade.
Retorno à normalidade: até um dia.

O Diretor responsável da Cooperativa irá verificar se o ambiente tecnológico está liberado, em condições confortáveis para o trabalho e confirmar com o departamento de TI/Fácil Informática, responsável por revisar se os principais serviços estão funcionando a nível de desempenho aceitável.

O funcionário responsável em conjunto com o agente de compliance e com a ciência do diretor responsável determinarão o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios, como as estruturas e estratégias que embasam o plano de continuidade de negócios possam ser atualizadas refletindo o ambiente de negócios atual da Cooperativa.

Havendo ocorrência de incidentes relevantes ou interrupções de serviços relevantes que configurem uma situação de crise, bem como das providências para o reinício das suas atividades, a Cooperativa irá comunicar o Banco Central do Brasil conforme determina o art. 22 da Resolução nº 4.658/18.

A Cooperativa, em atendimento as observações da Resolução, possui em seu contrato firmado com o prestador de serviço, cláusulas, mencionando os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada, para que as providências para a sua troca sejam tomadas, a fim de evitar futuros transtornos do reestabelecimento da operação normal da Instituição.

A Cooperativa definiu que serão realizadas anualmente sessões de divulgação a todos os funcionários e envolvidos no planejamento de continuidade de negócios no ambiente tecnológico, a fim de manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios vigente.
O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do plano, incluindo as alterações recentes.

Os testes têm por objetivo assegurar a eficiência e a efetividade do plano e deverão ser planejados (periodicidade) e executados a partir da data da sua implantação.
A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da coordenação/agente de controles internos e de riscos, com suporte da Tecnologia da Informação (prestadores de serviços contratados).

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela Diretoria e arquivado como documento de validação das estratégias por um período mínimo de 5 (cinco) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da Cooperativa.

12 – SERVIÇOS DE PROCESSAMENTO DADOS/ARMAZENAMENTO NUVEM

Conforme estabelecido em contrato, a empresa REZEK FERREIRA INFORMÁTICA LTDA**,** nome de fantasia **Fácil Informática,** é responsável pela gestão de segurança cibernética do sistema FacCred contratado pela **COOPERMSD** e pelo armazenamento dos dados em nuvem.

São hospedados utilizando a estrutura da Amazon AWS, empresa multinacional e líder mundial na prestação dos serviços de armazenamento em nuvem, com garantia de alta disponibilidade, sigilo, segurança e acessibilidade ao sistema e dados hospedados.

A gestão contratada não desonera a responsabilidade da Cooperativa, na qual deve também, indicar diretor responsável pelo gerenciamento da segurança cibernética na entidade que administra. O diretor indicado poderá exercer outras funções, desde que não haja conflito de interesse.

As empresas terceirizadas contratadas para efetuar os serviços de processamento de dados e armazenamento em nuvem podem representar riscos de cibersegurança. No caso da computação em nuvem, envolve riscos que são levados em conta pela Cooperativa, demandando assim cuidados proporcionais a esta identificação de ameaças.

A Cooperativa 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, plano de continuidade operacional, entre outros);

b) Verificação da capacidade do potencial prestador de serviços de forma a assegurar:

- Cumprimento da legislação e da regulamentação em vigor;
- Permissão de acesso da Cooperativa aos dados e as informações a serem processadas ou armazenadas pela empresa prestadora de serviços;
- Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviços;
- Aderência a certificações que a Cooperativa possa exigir para a prestação do serviço a ser contratado;
- Acesso da Cooperativa 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 Cooperativa por meio de controles físicos ou lógicos;
- Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos associados da Cooperativa.

Na avaliação da relevância do serviço a ser contratado por uma empresa terceirizada, a Cooperativa deverá considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo prestador de serviço, levando em conta, inclusive, a classificação dos dados e das informações quanto à relevância.
Todos os procedimentos e verificações deverão ser documentados.

No caso da execução de aplicativos por meio da internet, implantados ou desenvolvidos pelo prestador de serviço, a Cooperativa deve assegurar que a empresa terceirizada adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

A **COOPERMSD** deverá comunicar ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deverá ser realizada 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 Banco Central até 10 (dez) 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) 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 acima, a Cooperativa deverá solicitar autorização do Banco Central do Brasil para a contratação ou alteração contratual, observando o prazo mínimo de 60 (sessenta) dias antes da contratação ou alteração contratual.

A **COOPERMSD** 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.

Os contratos firmados entre a Cooperativa 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 clientes;

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

- Transferência dos dados ao novo prestador de serviços ou a Cooperativa;
- 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 **COOPERMSD** a:

- Informações fornecidas pela empresa contratada visando verificar o cumprimento dos itens 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 a Cooperativa 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 Cooperativa em decorrência de determinação do Banco Central do Brasil;

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

j) O contrato deverá 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 da resolução;

✓ A notificação prévia deve ocorrer também na situação em que a interrupção for motivada por inadimplência da Cooperativa.

Nota 1: Para reduzir a vulnerabilidade da **COOPERMSD** a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, a Cooperativa optou pelo armazenamento de seus dados e informações em nuvem, através da contratação de empresa especializada e devidamente habilitada.

A **COOPERMSD** é o **site principal** e a empresa **Fácil Informática**, é o site alternativo (**Backup**).

O site alternativo fica situado na cidade e estado de Belo Horizonte/MG e o canal de atendimento é feito por telefone (31-3319-1900), para disponibilizar o Backup do sistema Operacional da Cooperativa, relativo aos processos críticos de negócios das seguintes áreas:

a) Financeiro;

b) Cadastro;

c) Crédito;

d) Contabilidade.

Nota 2: A Cooperativa, em atendimento as observações da Resolução, possui em seu contrato firmado com o prestador de serviço, cláusulas, mencionando os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada, para que as providências para a sua troca sejam tomadas, a fim de evitar futuros transtornos do reestabelecimento da operação normal da Instituição. Outros critérios também, estão definidos em nossa política de gestão de serviços terceirizados.

Nota 3: Seguem alguns dados, informações e procedimentos adotados pela empresa Fácil Informática:

a) Possuem um NOC - Network Operations Center, responsável por monitorar preventiva e reativamente todos os ativos do ambiente do prestador de serviço. Possuem um CGSI - Comitê Gestor de Segurança da Informação, responsável por todas as questões e ações relacionadas à Segurança da Informação;

b) O ambiente fica hospedado em um único fornecedor (Amazon Web Services), acessível apenas por um Servidor Gateway TS. Todo ambiente é monitorado;

c) Fazem anualmente testes de invasão terceirizado (último feito com CLAVIS) com o objetivo de identificar e contornar vulnerabilidades não previstas pela equipe;

d) Proteção contra softwares maliciosos (antivírus, antimalware, outros): Apenas executáveis assinados com certificado confiável da Fácil podem ser executados no ambiente;

e) Criptografia: utilizam para senhas, no transporte de dados etc.

f) No que diz respeito à fase da implementação de código, utilizam as ferramentas para análise de código, revisão de código, realizam o desenvolvimento com metodologias orientadas ao teste, possuem testes unitários e de integração automatizados.

Nota 4: Outras informações do prestador de serviços, onde destacamos:
a) Prevenção a ataques de negação de serviço (DDoS - Distributed Denial of Service);
b) Prevenção de vazamento de informações (DLP - Data Loss Prevention);
c) Teste de intrusão (Pentest - Penetration Testing);
d) Análise de vulnerabilidades de sistemas;
e) Gestão de Acessos Lógicos;
f) Segmentação da rede de computadores / segregação de ambientes;
g) Análise de vulnerabilidades do ambiente;
h) Mecanismos de rastreabilidade, incluindo trilhas de auditoria e implementação de logs;
i) Manutenção de cópias de segurança dos dados e das informações;
j) Gestão de Correções (Patch Management);
k) Descarte Seguro de Equipamentos;
l) Network Access Control (NAC).

Nota 5: As políticas da Amazon de segurança compliance e SLA podem ser acessados nos links:
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
https://aws.amazon.com/pt/compliance/programs/
https://d1.awsstatic.com/legal/amazon-ec2-sla/Amazon_EC2_Service_Level_Agreement_-_Portuguese_Translation__2018-02-12_.pdf
https://d1.awsstatic.com/whitepapers/compliance/PT_Whitepapers/AWS_User_Guide_for_Financial_Services_in_Brazil.pdf

Nota 6: Conforme a divulgação do comunicado pelo Bacen sobre os países com os quais o Banco Central do Brasil tem convênio para intercâmbio de informações para fins de supervisão, os EUA, onde os dados estão hospedados estão na lista:
https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31999&tipo=Comunicado&data=10/5/2018

13 – DIVULGAÇÃO E REVISÃO

A política aprovada pela Diretoria, registrada em ata de reunião, está sendo comunicada aos funcionários, colaboradores, associados, empresa contratada de serviço em armazenamento em nuvem, prestadores de serviços relevantes para o necessário cumprimento, de forma a promover a disseminação da cultura na Cooperativa. Será divulgada através de comunicação verbal ou textual e na internet, no site da **COOPERMSD**.

A publicação (resumo) estará sendo divulgado ao público através da internet, no site da **COOPERMSD**, bem como, o documento físico encontra-se nas dependências da Cooperativa.

Esta Política, juntamente com o plano de ação e respostas a incidentes será revisada anualmente ou se houver mudança significativa, assegurando a sua contínua pertinência, adequação e eficácia.

14 – CONSIDERAÇÕES FINAIS

Os respectivos documentos referentes à política cibernética, plano de ação e de resposta a incidentes, relatório anual, contratos de prestação de serviços de processamento, armazenamento de dados e computação na nuvem, as informações compartilhadas e outros documentos pertinentes as exigências da legislação ficarão à disposição aos órgãos fiscalizadores pelo prazo de 5 (cinco) anos.

A Cooperativa, em atendimento à Resolução irá compartilhar as informações sobre os incidentes relevantes (o registro, a análise da causa e do impacto, o controle), inclusive as informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros.

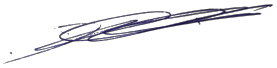
Todas as observações e ocorrências, assim como ações a serem aprimoradas para atualização desta política, serão inseridas em atas da Diretoria.

Declaramos que as respectivas política e documentos pertinentes foram aprovadas e registras em Atas na reunião da Diretoria realizada em 20/09/2021.

São Paulo/SP, 20 de setembro de 2021.

Electronically signed by:
Carlos Kanji Cesar Kamijo
Reason: Approved
Date: Sep 22, 2021 13:41 ADT

Carlos Kanji César Kamijo
Diretor Presidente



Electronically signed by:
Jose Angelo Francolin
Reason: Approved
Date: Sep 22, 2021 17:25 ADT

José Angelo Françolin
Diretor Administrativo

Electronically signed by:
Rubio Vinicius de Marcantonio
Reason: Approved
Date: Sep 22, 2021 13:48 ADT

Rúbio Vinicius de Marcantonio
Diretor Operacional

POLITICA SEGURANCA CIBERNETICA v20092021

Final Audit Report 2021-09-22

Created:	2021-09-21
By:	Janete Aparecida Rogante (janete_rogante@merck.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAltorGl-hjqQ6DFR3SPtu-CS3dZ-sthaN

"POLITICA SEGURANCA CIBERNETICA v20092021" History

Document created by Janete Aparecida Rogante (janete_rogante@merck.com)
2021-09-21 - 6:00:13 PM GMT- IP address: 155.91.45.236

Document emailed to Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com) for signature
2021-09-21 - 6:01:04 PM GMT

Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com) verified identity with Adobe Sign authentication
2021-09-22 - 4:41:06 PM GMT

Document e-signed by Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com)
Signature Date: 2021-09-22 - 4:41:06 PM GMT - Time Source: server- IP address: 155.91.45.242

Document emailed to Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com) for signature
2021-09-22 - 4:41:08 PM GMT

Email viewed by Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com)
2021-09-22 - 4:46:07 PM GMT- IP address: 155.91.45.236

Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com) verified identity with Adobe Sign authentication
2021-09-22 - 4:48:51 PM GMT

Document e-signed by Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com)
Signature Date: 2021-09-22 - 4:48:51 PM GMT - Time Source: server- IP address: 155.91.45.236

Document emailed to Jose Angelo Francolin (joseangelo_francolin@merck.com) for signature
2021-09-22 - 4:48:53 PM GMT

Jose Angelo Francolin (joseangelo_francolin@merck.com) verified identity with Adobe Sign authentication
2021-09-22 - 8:25:54 PM GMT

Document e-signed by Jose Angelo Francolin (joseangelo_francolin@merck.com)

Signature Date: 2021-09-22 - 8:25:54 PM GMT - Time Source: server- IP address: 155.91.45.239

Agreement completed.

2021-09-22 - 8:25:54 PM GMT