1. DEFINIÇÃO

Esta Instrução Normativa, devidamente aprovada pelo Conselho de Administração, estabelece os critérios a serem adotados pelos colaboradores, diretores e conselheiros da Cooperativa de Economia e Crédito Mútuo dos Empregados da CBMM Ltda, denominado Cooperativa, à resolução 4.893 de 26 de fevereiro de 2021, do Banco Central do Brasil, que estabelece a implementação da Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados de computação em nuvem.

2. OBJETIVO

Assegurar princípios e diretrizes básicas que garantam a integridade, confidencialidade, disponibilidade e autenticidade dos dados, observando o porte, o perfil de risco e os negócios desenvolvidos, a natureza das operações, a complexidade dos produtos, serviços, atividades e processos, assim como a sensibilidade dos dados e das informações sob responsabilidade da Cooperativa.

3. CAMPO DE APLICAÇÃO

As tarefas descritas nesta IN são aplicáveis a todos os colaboradores da Cooperativa, inclusive diretores e conselheiros, indistintamente, devendo ser observados os procedimentos para sua execução, e a mesma deverá ser revisada no mínimo anualmente.

4. RESPONSABILIDADES E AUTORIDADES

4.1 **Colaboradores Cooperativa:** É de obrigação de todas as áreas e colaboradores, executarem, observarem e cumprirem as normas que constam nesta IN.

4.2 **Diretoria Executiva:** Analisar e efetuar em conjunto com a Gerência da Cooperativa, a implementação e aquisição de novos sistemas, bem como acompanhar a área de TI na administração e controle da segurança de sistemas, computadores e rede. O Diretor Coordenador será responsável pela Política de Segurança Cibernética e pela execução do plano de ação e de resposta a incidentes.

Comunicar tempestivamente ao Banco Central do Brasil as ocorrências de

incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise, bem como as providências tomadas para o reinício das atividades.

4.3 **Conselho Administrativo:** É responsabilidade do Conselho de Administração aprovar, supervisionar e revisar, sempre que necessário, a presente política, garantindo a gestão de toda segurança cibernética da Cooperativa.

4.4 **Conselho Fiscal:** Acompanhar a execução desta IN.

4.5 **Gerência e Agente de Controle Interno:**

- Definir as permissões de acesso ao sistema, restringindo e controlando o acesso dos usuários;

- Administrar o acesso de usuários aos sistemas e máquinas de acordo com suas necessidades;

- Elaborar o relatório anual referente a implementação do plano de ação e de resposta a incidentes;

- Monitorar, em conjunto com a empresa responsável a infraestrutura de rede, realizando, periodicamente testes e varreduras no sistema que permitam identificar vulnerabilidades dos softwares de detecção de vírus e problemas/falhas no firewall da rede;

- Acompanhar, periodicamente, os relatórios de auditoria do sistema monitorando as ações realizadas, notadamente, aquelas vinculadas a criação e alteração de dados;

- Divulgar as linhas gerais da política de segurança cibernética, aos colaboradores, conselheiros, fornecedores e cooperados, atentando para uma linguagem clara e acessível a todos os públicos;

- Implementar programas de treinamento, cientificando e capacitando os colaboradores quanto a importância de manter a segurança da informação.

5. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

A Segurança da informação da Cooperativa estabelece os principais controles, denominados diretrizes:

• As informações da Cooperativa, dos cooperados e de todos envolvidos devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

• A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

• Todo processo, durante o seu ciclo de vida, deve 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.

• O acesso às informações e recurso só deve ser feito se devidamente autorizado.

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

• A concessão de acessos deve seguir critérios de menor privilégio, no qual os usuários têm acesso somente aos recursos e informações imprescindíveis para o pleno desempenho de suas atividades.

• A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

• Os riscos às informações da Cooperativa devem ser reportados ao Diretor que é responsável pela área de Segurança da Informação “BACEN”.

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

6. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

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

6.1 Gestão de Ativos da Informação:

6.1.1 Entende-se por Ativos da Informação todos os tipos de dados que se pode criar, processar, armazenar, transmitir, alterar e excluir. Podem ser tecnológicos

("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas).

6.1.2 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.

6.2 Classificação da Informação:

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

6.2.1 Confidencial: É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da Cooperativa. São protegidas, por exemplo, por criptografia. Dados confidenciais devem ser usados quando existe uma pessoa especifica que pode recepcioná-los.

6.2.2 Restrita: É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso à uma pasta ou diretório da rede.

6.2.3 Interna: Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da Cooperativa, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

6.2.4 Pública: São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

6.2.5 Sensível: Para as questões que envolvem a LGPD.

6.3 Gestão de Acessos:

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

6.3.2 Os acessos devem ser rastreáveis, a fim de garantir que ações sejam passíveis de auditoria e possam identificar individualmente o colaborador, para que seja responsabilizado por suas ações.

6.4 Gestão de Riscos:

6.4.1 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.

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

6.5 Tratamento de Incidentes:

Os incidentes de Segurança da Informação e cibernéticos da Cooperativa devem ser reportados à Diretoria.

6.6 Conscientização em Segurança da Informação:

A Cooperativa promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da informação. Dentro dos programas de treinamento e capacitação de membros estatutários e colaboradores, a cooperativa incluirá a segurança cibernética como programa de capacitação. Na prestação de informações a clientes e usuários sobre precaução na utilização de produtos e serviços financeiros, os colaboradores serão orientados sempre na prestação dos atendimentos e as informações e orientações no trato desses serviços, que são protegidos pelo sigilo previstos na Lei Complementar 105/2001. Em relação ao comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética, a diretoria da cooperativa deverá estar atualizada no que ocorre na área de segurança cibernética, atuando preventivamente, cobrando informações e providências, além de ter um diretor indicado responsável pela segurança cibernética.

6.7 Segurança Física do Ambiente:

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

7. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

7.1 Ações a serem desenvolvidas:

Realização de gestão de risco através de um processo estruturado que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoramento dos riscos que podem afetar negativamente os negócios da Cooperativa.

7.2 Rotinas, Procedimento e Controles a serem utilizados na Prevenção e Resposta a Incidentes:

No intuito de garantir a efetividade da Política de Segurança Cibernética, a Cooperativa deve implementar as seguintes ações:

a) Monitorar em conjunto com a empresa responsável a infraestrutura de rede, realizando, periodicamente, testes e varreduras no sistema que permitam identificar vulnerabilidades dos softwares de detecção de vírus e problemas/falhas no firewall de rede;

b) Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

c) Monitorar as rotinas de backup, executando testes regulares de restauração dos dados.

d) Manter e assegurar os recursos tecnológicos necessários para garantir o desempenho das atividades executadas, sempre com segurança.

Eventos, mesmo que suspeitos, deverão ser analisados e validados rapidamente. Uma vez confirmada a ocorrência de um incidente, então a análise do escopo do incidente deverá ser executada. Essa análise deverá prover informações suficientes que permitam identificar e priorizar as atividades subsequentes;

Todos os usuários serão responsáveis por relatar qualquer tipo de eventos e fragilidades que possam causar danos à segurança cibernética.

7.3 Resposta a Incidentes:

A atividade de resposta a incidentes compreende as seguintes reações:

a) A partir da detecção de um incidente, é importante controlá-lo antes que uma possível extenção comprometa outros recursos;

b) A estratégia de resposta ao incidente a ser adotada deve ser baseada no tipo (Ex: vírus, perda de arquivo, incêndio, etc) e na criticidade do incidente (Ex: impacta na imagem ou nas operações da Cooperativa, compromete várias áreas, entre outros);

c) Após a identificação e a confirmação do incidente, a resposta deverá ser realizada a partir das seguintes ações:

- Preservar, na medida do possível, todas as evidências, para que seja possível identificar o problema e rastrear a possível causa;
- Agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;
- Utilizar todos os recursos necessários para a implementação de uma estratégia de reação, seja ela permanente ou provisória.

7.4 Área Responsável pelo Registro e Controle de Incidentes Relevantes:

O Agente de Controles Internos da Cooperativa será o responsável pelos registros e controles de incidentes bem como a resposta dada a estes incidentes. Deverá também, preencher o Relatório Anual de Plano de Ação e Resposta a Incidentes, com data base de 31 de dezembro. Anexo I desta IN.

O relatório deverá abordar no mínimo:

a) a efetividade da implementação das ações desenvolvidas para adequar a estrutura organizacional e operacional da Cooperativa aos princípios e diretrizes da política de segurança cibernética;

b) as rotinas procedimentos, controles e tecnologias a serem utilizados na prevenção e resposta a incidentes;

c) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

d) os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

8. CONTINUIDADE DOS NEGÓCIOS

A Cooperativa procurará investigar os eventos e incidentes de forma a não influenciar a continuidade dos negócios, principalmente no caso de interrupção de serviços relevantes, primando assim pela execução normal das atividades da instituição o mais breve possível, de forma que a interrupção não ultrapasse 24 (vinte e quatro) horas. Alguns cenários de incidentes que podem influenciar a continuidade dos negócios são: vazamento de dados/informações,

indisponibilidade de recursos computacionais, quebra de integridade dos dados via alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados, fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da instituição. A Cooperativa deverá fazer comunicação ao Banco Central dos procedimentos adotados para continuidade dos negócios em caso de ocorrência de incidentes relevantes e das interrupções dos serviços relevantes, que venha a afetar o funcionamento normal de suas atividades que configurem uma situação de crise pela instituição financeira.

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

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

O contrato foi firmado com a empresa Rezek Ferreira Informática ltda – Fácil Informática e terá todo o sistema faccred – e os dados operacionalizados por ele – hospedados em datacenter com disponibilidade de tempo (99,97%), em nuvem, utilizando a estrutura da empesa Amazon.

9.1 Normas Gerais:

A hospedagem em nuvem dispensa a aquisição de licenças dos softwares de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem;

A empresa contratada realizará o backup em nuvem, totalmente automatizado, em ambiente de alta disponibilidade e durabilidade, com garantia da integridade dos dados por meio de restaurações periódicas em ambiente de homologação e confidencialidade das informações;

A empresa contratada monitorará o banco de dados, incluindo o dimensionamento, instalação e configuração até tuning, backup/recover, monitoramento e aplicação de patches;

A empresa contratada realizará o monitoramento de servidores e serviços, notificando em caso de falhas, mantendo características proativas (ações para antecipação de falhas), reativas (ações de respostas a eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas);

A empresa contratada deverá implementar e manter controles de segurança incluindo, sem limitação, segurança de hardware e software, firewalls, filtros e outras ferramentas de segurança;

A empresa contratada se responsabilizará por armazenar e transmitir as credenciais de acesso e demais informações confidenciais de maneira criptografada;

A empresa contratada deverá garantir a segregação de acesso entre os ambientes de seus diferentes clientes, impedindo o acesso não autorizado às informações;

Caberá à empresa contratada disponibilizar informações para auditorias (internas e externas) e investigações judiciais quando solicitadas;

O Backup,deverá ser realizado de acordo com a periodicidade abaixo descrita, mantendo cada um dos backups efetuados sob a política cíclica de armazenamento, que garante a disponibilidade de restauração de backup dos 7 (sete) últimos dias, com as seguintes características:

- Backup diário de todo o Banco de Dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,9999999% de durabilidade e de 99,97% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais; e

- Para garantir a sua integridade, os backups serão testados semanalmente.

9.2 Este Serviço em Nuvem Compreende:

- Ferramentas para governança e rastreabilidade de dados;

- Atendimento às exigências legais uma vez que o trabalho da Amazon é realizado em conjunto com órgãos externos de certificação e auditores independentes para fornecer aos clientes informações importantes sobre suas políticas, processos e controles;

- Ferramentas simples e avançadas que permitem a CREDMAIS determinar onde seu conteúdo será armazenado, proteger o conteúdo em trânsito e em repouso e gerenciar o acesso a serviços e recursos da Amazon;

- Políticas e procedimentos formais para estabelecer parâmetros comuns aos funcionários sobre os padrões e diretrizes de segurança da informação. A política do sistema de gerenciamento de segurança da informação da Amazon estabelece diretrizes para proteger a confidencialidade, integridade e disponibilidade dos sistemas e conteúdo dos clientes;

- Opção de analisar e fazer download de relatórios e detalhes sobre os controles de segurança usando o portal automatizado de relatórios de conformidade

disponível na Console de Gerenciamento da Amazon;

- Ferramentas para monitorar anormalidades e verificar notificações de segurança;
- Identificação e separação lógica dos dados do Cliente em nuvem;
- Curso on-line gratuito desenvolvido para apresentar os fundamentos da computação e segurança em nuvem.
- Existência de acordos para a troca de informações entre o Banco Central do Brasil e as autoridades dos países onde os serviços da Amazon podem ser prestados, não causando danos à operação regular da Cooperativa, nem constrangimento à performance do Banco Central do Brasil.

10. COMUNICADOS

A presente IN 014 – Política de Segurança Cibernética deverá ser divulgada a todos os colaboradores da Cooperativa, Conselheiros, Diretores, bem como a todas as empresas prestadoras de serviços terceirizados.

11. ANEXOS

Anexo I – Relatório Anual Plano de Ação e Resposta a Incidentes (Modelo)

Anexo II – Histórico de Revisões

12. VIGÊNCIA

A presente Instrução Normativa entra em vigor em 19/04/2023.

Jose Vander Firmino Gonçalves
Diretor Financeiro

Marco Antonio de S. Vieira
Diretor Coordenador

Anexo I

RESOLUÇÃO 4893/2021 - RELATÓRIO ANUAL DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES

DATA BASE DO RELATÓRIO.: ____/_____/_____

	AÇÃO	FREQUÊNCIA	RESPONSÁVEL	STATUS
Controle de acesso	Avaliar junto aos colaboradores da Cooperativa se as senhas (Sistema Fácil, rede, arquivos relevantes e outros sistemas) estão sendo alteradas trimestralmente	TRIMESTRAL	Agente de Controles Internos	
Segurança & Tratamento da Informação	Verificar junto a empresa Fácil Informática se o backup do sistema está sendo efetuado conforme periodicidade definida na IN - 014	TRIMESTRAL	Agente de Controles Internos	
	Verificar junto a área de T.I se estão sendo realizados backups dos arquivos armazenados (Word, Excel, PDF, JPG e Outros)	TRIMESTRAL	Agente de Controles Internos	
	Verificar junto a área de T.I se os softwares de proteção estão sendo atualizados e se estão sendo realizados testes e varreduras que permitam identificar vulnerabilidades	TRIMESTRAL	Agente de Controles Internos	
	Verificar junto a área de T.I se está sendo efetuado controle de tráfego de dados através do firewall (por máquina)	TRIMESTRAL	Agente de Controles Internos	
	Realizar controle de acesso dos prestadores de serviços/terceiros	QUANDO NECESSÁRIO	Gerência	
Melhoria Contínua	Registrar os incidentes ocorridos estabelecendo plano de ação e executar as ações para tratativa	TRIMESTRAL	Agente de Controles Internos	
	Realizar levantamento de necessidade de investimentos, com objetivo de melhorar a segurança e organização dos dados da Cooperativa e de seus clientes	SEMESTRAL	Agente de Controles Internos	

INCIDENTE	DATA	ORIGEM	CRITICIDADE	TIPO IMPACTO	TEMPO MÍNIMO RESPOSTA	AÇÃO	RESPONSÁVEL	STATUS	RESULTADOS OBTIDOS

CONSELHO DE ADMINISTRAÇÃO **DIRETOR RESPONSÁVEL** **AGENTE DE CONTROLE INTERNO**

VERSÃO	ITEM	HISTÓRICO DA REVISÃO	DATA DA REVISÃO
1.0	Todos	Emissão do documento com aprovação do Conselho de Administração da Cooperativa através da Ata de nr 01/2021.	26/01/2021
2.0	Todos	Emissão do documento com revisão geral e adequação para atendimento ao apontamento 114.1 do RAC exercício ano de 2022, com aprovação do Conselho de Administração da Cooperativa através da Ata de nr 04/2023.	19/04/2023