Política de Segurança Cibernética e da Informação

Estado: Vigente	
Aprovado: AGOE 2020	Data: 11-03-2020
Versão VI Março/23	Aprovado na Ata CA 410

- **Atribuições**

Este documento tem como objetivo estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos que tangem as informações acessadas pelos administradores, funcionários e/ou outros colaboradores da C.E.C.M. Minuano na sua atuação interna e externa.

A Cooperativa incorpora em seus valores a convicção de que o exercício de suas atividades e a expansão de suas atividades devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus colaboradores. Na constante busca de seu desenvolvimento e da satisfação de seus associados, a Cooperativa busca transparência e cumprimento da legislação aplicável às atividades as atividades de administração e gestão dos recursos de seus associados.

A publicação desta Política representa o compromisso de todos os colaboradores da instituição com os valores e as práticas fundamentais na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento da Cooperativa e a defesa dos interesses dos clientes estarão sempre pautadas nas diretrizes expostas nessa Política.

A área de Riscos e Controles Internos é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados com os níveis adotados pela Cooperativa.

A área de Riscos e Controles Internos está apta a detectar eventuais desvios de conduta que possam colocar em Risco: associados, colaboradores, terceiros. As políticas, manuais e estatuto estão disponíveis para fácil acesso e visualização do público, e o diretor responsável atua de forma direta no incentivo e estímulo da leitura e atualização do documento.

A Cooperativa estimula e oferece capacitação e treinamento contínuo, com o objetivo de desenvolver e aprofundar os conhecimentos necessários para auxiliar no processo de segurança da informação. E após esse processo a equipe passa por uma avaliação buscando medir o aproveitamento e os conhecimentos adquiridos.

- **Importância da Segurança da Informação**

Os pilares da segurança da informação nos dão subsídios para proteger as informações da Cooperativa Minuano. Portanto, quando mencionamos segurança

da informação estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como controles de acesso, vigilância, contingência de desastres naturais, contratações clausulas e demais questões que juntas formam uma proteção adequada para qualquer empresa. (ISO 27002 A.5.1.1)

- **O que é Política de Segurança da Informação?**

Política de Segurança é um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável. (ISO 27002 A.5.1.1)

- **A informação é só o que está nos sistemas?**

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes e externos da cooperativa.
Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio. (ISO 27002 A.5.1.1)

- **Princípios da Segurança da Informação**

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamento, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos. (ISO 27002 A.5.1.1)

- **Confidencialidade**: Proteção da informação compartilhada contra acesso não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

- **Integridade**: Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma

pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

- **Disponibilidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

- **Acesso Controlado**: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

- **Regras do Uso de Tecnologia**

- Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na Cooperativa ou para outras situações formalmente permitidas. (ISO A.6.1.3)
- Quando o usuário se comunicar através de recursos de tecnologia da Cooperativa, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa.
- Os conteúdos acessados e transmitidos através de recursos de tecnologia da Cooperativa devem ser legais, de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário. (ISO A.15.1.5)
- O uso dos recursos de tecnologia da Cooperativa pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente.
- Cada usuário é responsável pelo uso de recursos que lhe forma fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados. (ISO A.6.1.3)
- Os recursos de tecnologia da Cooperativa, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização. (ISSO A.6.1.3)
- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Riscos e Controles Internos (ISO A.13.1.1)

- **Regras do Uso do Computador**

- O computador disponibilizado para o usuário é de propriedade da C.E.C.M. Minuano;

- O computador disponibilizado para o usuário tem por objetivo o desempenho das atividades profissionais desse usuário na organização;
- É necessário que o Gestor do usuário o autorize a usar o computador. Deve ser feita uma solicitação à área de infraestrutura, que autorizará tecnicamente e fará a liberação mediante a disponibilidade de recursos (ISO A.7.1)
- Todos os equipamentos, softwares e permissões acessos devem se testados, homologados e autorizados pela área de infraestrutura para uso da Cooperativa. (Isso A.10.3)
- A Cooperativa pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário. (ISO A.10.3)
- Cada computador tem o seu gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área de infraestrutura. (ISO A.7.1)
- A identificação do usuário ao computador é feita através do login e senha disponibilizado pela área de Infraestrutura, portanto ela é sua assinatura eletrônica.
- Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura. (ISO A.7.1)
- Não é permitido aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura, assim como implantar ou alterar componentes físicos no computador.
- A Cooperativa verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pela área de infraestrutura e Compliance.
- É responsabilidade de cada usuário cuidar de seu equipamento, garantir sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de infraestrutura.
- Todas as práticas que representam ameaças à segurança da informação serão tratadas com a aplicação de ações disciplinares.
- O usuário é responsável por todo acesso realizado com a sua autenticação.
- O usuário é proibido de acessar endereços de internet (sites) que:

* Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
* Possuam conteúdo imoral.
* Contenham informações que não colaborem para o alcance dos objetivos da Cooperativa Minuano.
* Defendam atividades ilegais. Menosprezem, depreciem ou incitem o preconceito a determinadas ou gêneros.
* O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor de sua área.

- É proibido o uso de serviços de mensagem instantânea através dos computadores da Cooperativa, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pelo Compliance.
- É proibido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores da Cooperativa, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pela área de infraestrutura.
- Periodicamente a área de infraestrutura revisará e bloqueará o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Empresa.
- É proibido o acesso aos serviços de correio eletrônico particular, tipo webmail, através dos recursos de tecnologia da Cooperativa Minuano.
- A Cooperativa disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais (ex.: usuário@cooperativaminuano.com.br).
- O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Cooperativa.
- Se houver necessidade de troca de endereço, a alteração deverá ser autorizada pela área de infraestrutura e registrada para possibilitar uma posterior verificação da auditoria.
- As caixas postais de contas de correio eletrônico da Cooperativa Minuano têm limite de tamanho de 3.2GB e as mensagens enviadas/recebidas poderão conter arquivos com até 10MB por mensagem.
- O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da Cooperativa Minuano.
- Em situações autorizadas pela Gerência, as mensagens do correio eletrônico de um usuário poderão ser acessadas pela Cooperativa Minuano ou por pessoas por ela indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal.

O usuário que utiliza um endereço de correio eletrônico:
- É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.
- Pode enviar mensagens necessárias para o seu desempenho profissional na Empresa.
- É proibido criar, copiar ou encaminhar mensagens ou imagens que:

* contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.
* Façam parte de correntes de mensagens, independente de serem legais ou ilegais.
* Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não.
* Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, idade, religião....

* Possuam informação imprópria para o ambiente de trabalho.
* Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros,
* Defendam ou possibilitem a realização de atividades ilegais.
* Sejam ou sugiram a formação ou divulgação de correntes de mensagens.
* Possam prejudicar a imagem da Cooperativa Minuano.
* Sejam incoerentes com o Código de Ética.

Deve ser diligente em relação:

- Aos usuários que receberão a mensagem,
- Ao nível de sigilo da informação contida na mensagem,
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantido a confidencialidade dos mesmos
- Não abra mensagens de origem desconhecida;

Deve deixar mensagem de ausência quando for passar um período maior do que 48 horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

- **Cópia de Segurança**

O backup do sistema (Fácil) é realizado diariamente de forma automática de acordo com o horário programado, o qual, atualmente tem horário de conclusão previsto para as 23h15min.
O arquivo de backup abrange toda a base de dados existente no sistema FacMútuo (Fácil), contemplando as informações de todos os módulos (Empréstimo, Contabilidade, Capital, Convênios, imobilizado, entre outros).
O backup realizado de forma automática é armazenado no diretório Y:\MINUANO no ambiente disponibilizado pelo fornecedor (Fácil).
Além do armazenamento automático realizado no ambiente do fornecedor (Fácil), diariamente a Cooperativa, por meio do Assessor de TI, realiza a cópia do arquivo completo de backup para a rede interna da Cooperativa. Este arquivo é salvo no computador do Assessor de TI, no qual são mantidos, além do arquivo referente ao último dia, versões de todos os dias da semana atual, da última semana e versões com o fechamento de cada mês e ano.
Já os arquivos tratados pela Cooperativa que não fazem parte do sistema/banco de dados, tais como e-mails, planilhas auxiliares, formulários preenchidos, orçamentos, entre outros documentos armazenados no servidor interno da Cooperativa, são salvos diariamente em backup em mídia externa (SSD externo).
Este backup é realizado automaticamente pelo sistema diariamente às 20h30min.
Todos os dias é substituído o SSD Externo conectado ao servidor.
Ao término do expediente da Cooperativa, o SSD externo contendo o backup anteriormente citado é retirado da sede da Cooperativa pela Gerente ou pelo Assessor de TI, retornando-o para a sede no próximo dia de expediente.

Além do backup do dia anterior, também ficam salvos no SSD externo arquivos com versões anteriores dos arquivos.

- **Regras do Uso do Telefone**

- A Cooperativa Minuano disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais.
- Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela área de TI e registrada para possibilitar uma posterior verificação de autoria.
- O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade da Cooperativa Minuano.
- É proibido utilizar o telefone para conversas que:
* contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
* Menosprezem, depreciem ou incitem o preconceito a determinadas classes.
* Possuam informação imprópria para um ambiente profissional;
* Defendam ou possibilitem a realização de atividades ilegais;
* Possam prejudicar a imagem da Cooperativa Minuano;
* Sejam incoerentes com o Código de Ética.

- **Linhas Gerais de Comportamento**

- Falar sobre informações restritas ou segredos profissionais em um lugar público ou por telefone merecem cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa.
Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa da empresa. Qualquer pendrive ou conexão de rede pode conter dados valiosos.
- O lixo pode ser uma fonte de informações para pessoas mal-intencionadas.
Fragmente os documentos que contenham informações sensíveis, pessoais ou da Cooperativa Minuano antes de descartá-los.
- Cada tarefa desenvolvida na Cooperativa Minuano precisa ter um responsável.
A única forma de saber o responsável por cada atividade é através da identificação do usuário. Tudo que é feito com a sua identificação (assinatura ou senha) é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está usando esse acesso. Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua.

***A área de Infraestrutura de TI é responsável por liderar anualmente os processos de revisões de acessos físicos ou lógicos de todos os colaboradores da Cooperativa Minuano e propor a alteração e sua respectiva implementação.

Quaisquer dúvidas relacionadas com a presente política devem ser esclarecidas com a Gerência e com a área de Infraestrutura de TI.

- **Plano de Ação e de Resposta a Incidentes**

1. DOCUMENTO

O Plano de Ação estabelece as expectativas da cooperativa em implementar melhorias e novas funcionalidades na operação diária. E o relatório de Resposta a Incidentes estabelece ações desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional frente aos incidentes ocorridos. Assim esses documentos atuam juntamente aos princípios e às diretrizes da política de segurança cibernética.
O presente Plano foi aprovado pela Gestão e Diretoria Executiva, sendo nomeada a Gestão a atuar na liderança e execução dos processos, bem como realizar as ações para a criação e manutenção das condições necessárias ao desempenho das atividades e responsabilidades previstas neste Plano.

A instituição elabora um relatório anual sobre a implementação do plano de ação e de respostas a incidentes, o resumo do resultado obtido na implementação das rotinas, os incidentes relevantes e resultado dos testes de continuidade de negócio. As informações são documentadas e revisadas anualmente com data-base de 31 de dezembro ou conforme a necessidade.

2. INSTRUÇÕES

O plano é elaborado detalhando vários tipos de eventos ou riscos operacionais externos, com isso, ocorre o acompanhamento das operações e rotinas diárias visando minimizar os eventos mais comuns como:

Atos de Vandalismo;
Incêndios;
Ameaças de Bombas;
Roubos;
Interrupção do Fornecimento de Serviços Telecomunicação;
Interrupção do Fornecimento de Energia Elétrica;
Inundações; e
Outros, a critério da administração da instituição.

- **Cenários de Risco**

CENÁRIOS DE RISCO		
1.	NOME DO RISCO	Risco de Incêndio, Danos Elétricos, Roubo e/ou Furto, Queda de Aeronaves e Risco de Raio e Explosão de Qualquer Natureza.
2.	LOCAL	Rua Gonçalves Dias, nº 88 salas 1005 e 1006, Canoas
3.	DESCRIÇÃO	Sede Cooperativa Minuano
4.	FATORES CONTRIBUINTES	Sinistro
5.	RESULTADOS ESTIMADOS	Dano Parcial/Total de Material e Equipamentos de Trabalho dos Colaboradores da Cooperativa Minuano.

- **Operação**

4.1. IDENTIFICAÇÃO DOS RISCOS

- Risco de Incêndio;
- Risco de Danos Elétricos;
- Risco de Roubo e/ou Furto;
- Queda de Aeronaves;
- Risco de Raio e Explosão de Qualquer Natureza

- **Monitoramento**

Atualmente o monitoramento do prédio é feito por câmeras e alarmes. A portaria fica responsável pela comunicação ao responsável da Cooperativa, em caso de movimentação suspeita, indícios de incêndio, ou qualquer possibilidade de risco para as dependências e colaboradores presentes no local.

- **Alarme**

O prédio da Sede da Cooperativa Minuano possui Alarme de Incêndio, cujo monitoramento é realizado pelo zelador.

- **Acionamento dos Recursos**

Atualmente a Cooperativa possui um Contrato de Seguro com HDI Seguros, para a Sede Administrativa. Sua base de dados é composta por Backups. Um desses Backups (Sistema e Arquivos Internos da Cooperativa) fica aos cuidados da Gestão da Cooperativa Minuano, que diariamente o retira das dependências. Em sua ausência fica o Assessor de TI (Tecnologia da Informação)

responsável por tal procedimento. O outro Backup corresponde a um Contrato com a Fácil Informática, cujo banco de dados do sistema possui armazenamento (Hospedagem) em nuvem. (nº CT-NUV-19436-2018)

- **Mobilização e deslocamento dos Recursos**

Mediante contato com HDI Seguros (Proposta 18408840), será comunicado sinistro para que se tome as medidas providências.

Os colaboradores da Cooperativa Minuano serão alocados à unidade mais próxima (Pac Canoas - Sede AGCO), onde desempenharão suas atividades até que a situação na sede possa estar regularizada.

Será comunicado ao Bacen no prazo de 24hrs sobre a ocorrência do Sinistro e as providências a serem tomadas para o reinício das atividades.

A cooperativa também comunicará aos associados e colaboradores (via e-mail, intranet, site, telefones...) sobre a ocorrência do sinistro e prazo para regularização.

- **Retorno às atividades**

Após a regularização das condições da Sede, mediante contato com a seguradora, e disponibilização das instalações, serão restaurados backups de arquivos do sistema, possibilitando retorno às atividades da Sede da Cooperativa.

- **Revisão**

Testes de Backup

O arquivo de backup do sistema é testado de forma semestral, em ambiente de Homologação do Fornecedor (Fácil), quando, mediante solicitação, a base de testes (Homologação) é ativada com a base de uma determinada data.

Backup no site de contingência
Método do backup e ferramenta utilizada:

O backup local é sincronizado com o servidor contingência do sistema que fica no site remoto.

Frequência do backup para o site de contingência:
Backup diário

**O Banco Central do Brasil poderá vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, quando constar, a qualquer tempo, a inobservância do disposto nesta

Resolução, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

Aprovado na Assembleia Geral de 11 de março de 2020. Revisado e aprovado pelo Conselho de Administração ata n°410 em 24 de março de 2023.

Cláudio Luís Schwade
Diretor Presidente

Luiz Antonio Hüttner
Diretor Financeiro

Wilmar Schroeder Junior
Diretor Administrativo