



POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS PROFESSORES ESTADUAIS DA REGIÃO
METROPOLITANA DE PORTO ALEGRE – EDUCREDI

Ano/Versão	Ata Aprovada	Modificação	Responsável
2019	30/2019	Aprovação	Caroline Hernandez
2020 – I.	49/2020	Revisão e Implementação de acordo Resolução Bacen N° 4.658	Caroline Hernandez
2023 - II	84/2023	Resolução Bacen N° 4893	Caroline Hernandez

1. OBJETIVO

O objetivo desta política é estabelecer as diretrizes necessárias para assegurar a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pelo Cooperativa Educredi, de acordo com o seu porte e responsabilidades.

Nesta política, 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 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 de administração e gestão dos recursos de seus associados.

A publicação desta, representa o compromisso de todos os colaboradores da instituição com valores e práticas fundamentais na integridade, confiança e lealdade. Portanto a contante busca do desenvolvimento da Cooperativa e a defesa dos interesses nessa Política.

2. ABRANGENCIA

A Política de Segurança Cibernética e da Informação abrange toda a Cooperativa e suas áreas de negócios, destinando-se a todos os colaboradores, estagiários, terceiros e prestadores de serviços, visando a abrangência de todos que manuseiam dados ou informações sensíveis à condução das atividades operacionais da organização.

3. PRINCIPIOS E DIRETRIZES - 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 é considerado inaceitável.

Entende-se por informação toda e qualquer conteúdo ou dado que tenha valor para 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 nos externos da Cooperativa. Por isso todo cuidado é pouco na hora de imprimir relatórios, jogar papeis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas (ISO27002 A 5.1.1).

O processo de Segurança Cibernética, cujo objetivo é proteger as informações do negócio e clientes, é pautado pelos princípios fundamentais de:

- Confidencialidade: quando o acesso à informação deve ser disponibilizado apenas para as entidades ou pessoas devidamente autorizadas pelo proprietário ou dono da informação;
- Integridade: fato de manter a informação armazenada e trafegada com todas as suas características originais ao longo do seu ciclo de vida estabelecidas pelo proprietário ou dono da informação;
- Disponibilidade: garantir que a informação esteja disponível para uso sempre que entidades ou pessoas autorizadas necessitem.

- 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. Ameaça à segurança ocorre quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

As diretrizes estabelecem um programa de prevenção, detecção e redução de vulnerabilidades e impactos relacionados aos incidentes cibernéticos.

4. EDUCREDI - SEGURANÇA DA INFORMAÇÃO

4.1 Regras para 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 (ISSO 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 de que não comprometa a imagem da empresa. Os conteúdos acessados e transmitidos 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 da tecnologia da Cooperativa devem ser legais, de acordo com o Código de ética, e devem contribuir para as atividades profissionais do usuário (ISSO A.15.1.5).

O uso dos recursos de tecnologia da Cooperativa pode ser encaminhado, auditado ou verificado pela empresa, mediante a 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 (ISOA.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 (ISOA6.1.3). Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à Gestora, que faz a gestão dos riscos e controles internos.

4.2 Regras do Uso do Computador/ Notebooks

O computador disponibilizado para o usuário é propriedade da Cooperativa Educredi e tem por objetivo o desempenho das atividades profissionais. É necessário que o Gestor autorize o uso do computador, através uma solicitação, abrindo chamado à área de infra (Prestador de Serviços), que autorizará tecnicamente, formatando de acordo com o solicitado ou função do colaborador (sistema operacional, ferramentas e demais aplicativos necessários) - (ISSO.A 7.1).

Não é permitido aos usuários implantar novos programas ou alterar configurações sem permissão formalizada a Infraestrutura e Gestor direto, assim como implantar ou alterar os componentes físicos. É responsabilidade de cada usuário cuidar de seu equipamento, garantir sua integridade física e seu perfeito funcionamento seguindo as regras e orientações pela gestora.

Todos os equipamentos, softwares e permissões de acessos devem ser testados, homologados e autorizados pelo Diretor para uso da Cooperativa (ISSO.A.10.3).

Em qualquer momento a Cooperativa poderá retirar, substituir o computador disponibilizado para o usuário (ISOA.10.3). A identificação do usuário ao computador é feita através de login e senha disponibilizado pela área de infraestrutura portanto ela é sua assinatura eletrônica.

A cooperativa verifica regulamente 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 Gestor. 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. Usuário é proibido de acessar endereços de internet (sites) que: possam violar direitos de autor, marcas, licenças de programas ou patentes existentes; possuam conteúdos morais; contenham informações que não colaborem para o alcance dos objetivos da Educredi. Assim como conteúdos de atividades ilegais, que menosprezem, depreciem ou incitem o preconceito a determinadas ou gêneros.

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 e pela área de T.I. Proibido também o acesso de serviços de Correio eletrônico particular, tipo webmail, através dos recursos de tecnologia da Cooperativa Educredi.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e que o uso do material foi autorizado pelo gestor de sua área.

Periodicamente a área de infraestrutura revisará e bloqueará o acesso para os endereços da Internet que não estejam alinhado com esta Política e com o Código de Ética da Cooperativa.

A Educredi disponibiliza endereços de correio eletrônico para utilização do usuário focado na área que desempenhará suas atividades profissionais no período de vínculo com a Educredi. Em casos que houver a necessidade de troca, esta alteração deverá ser concedida pelo Gestor e área de Infraestrutura e registrada para fins de auditoria.

As Caixas postais de contas de correio eletrônico da Cooperativa têm o limite de 1.6 GB e as mensagens as mensagens enviadas/recebidas poderão conter arquivos com até 10MB por mensagem associadas a esse endereço são de propriedade da Educredi.

Em algumas situações autorizadas pela Gerência, as mensagens do Correio eletrônico poderão ser acessadas pela Educredi 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 das mensagens e uso relativos ao seu Email. 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 ofensiva de qualquer natureza ou ainda participar de correntes. Mensagens que depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, idade ou religião.

4.3. Backup

Todos nossos backups são automatizados por sistemas para que seja realizado um Backup Completo. Todos nossos arquivos e sistemas possuem backup em nuvem.

O backup do sistema (Faccred/Fácil) é de responsabilidade da empresa contratada (Faccred/Fácil Informática) no qual:

- a) todos os módulos licenciados do SISTEMA, não a necessidade de instalação de *softwares* nas estações-clientes da Cooperativa e com a dispensa de aquisição de licenças dos *softwares* de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem;
- b) realização de *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.

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:

- acompanhamento do banco de dados, contemplando desde o dimensionamento, instalação e configuração até *tuning*, *backup/recover*, monitoramento e aplicação de *patches*; e,
- monitoramento de servidores e serviços, com notificações em caso de falhas, com características Proativas (ações para antecipação de falhas), Reativas (ações de resposta a eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas);
- *backup* diário de todo o Banco de Dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,9999999% de durabilidade e de 99,95% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais; e,
- *os backups* serão testados semanalmente (restauração em ambiente de homologação) para garantir sua integridade;

Além dos procedimentos de segurança dos dados a que alude o subitem anterior, a Faccred/Fácil Informática disponibilizará, sob demanda, um arquivo contendo o backup lógico do banco de dados sempre que solicitado. Por questões de segurança, este arquivo será disponibilizado através de conexão criptografada, no formato EXPDP do Oracle, compactado através de ZIP e protegido por uma chave de segurança.

Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

A cooperativa Educredi conta com os serviços em Nuvem da Empresa Fácil Informática, instalados em 05/2020, de acordo com as cláusulas contratuais assinada entre as entidades.

Os serviços em nuvem da cooperativa atendem corretamente aos pontos desta política, sendo a empresa Fácil Informática de fácil contatação, inclusive se responsabiliza por informações caso as auditorias solicitem, assim como prestar informações ao Bacen.

A empresa Fácil Informática possui seus processos internos em caso de instabilidade no acesso ao sistema. É tratado internamente e posteriormente é instruído aos seus clientes os procedimentos necessários para acessar o sistema novamente, não existindo longos períodos sem acesso ao mesmo, prazo de 24 horas para retorno. Em caso de necessidade de migração de dados para outra empresa do ramo, a fácil possui a base pronta, sendo necessário somente a comunicação a mesma.

Os arquivos da Cooperativa, arquivos internos, que não fazem parte do sistema/banco de dados, tais como e-mails, planilhas auxiliares, formulários, orçamentos, entre outros documentos, a Educredi faz a migração dos arquivos internos para Nuvem da Microsoft passando a utilizar OneDrive. Esses procedimentos em nuvem viabilizam restaurações de arquivos de até 30 dias.

4.4. Regras do Uso do Telefone

A Cooperativa disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais. E todas as informações, conversas associadas a esse número são de propriedade da Educredi. Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela Gestão e Diretoria Executiva.

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 Educredi; sejam incoerentes com o Código de Ética.

4.5 Demandas Externas

Quando necessário e, para atender demandas e necessidades pontuais da Instituição, deverá constar nos contratos, uma cláusula de confidencialidade ou a formalização assinada de um Termo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela Instituição.

4.6 Registro e Respostas de Incidentes de Segurança

Os incidentes de segurança cibernética relevantes são registrados, bem como deve ser realizada a análise das suas causas e dos impactos deles decorrentes.

No caso da ocorrência de incidentes relevantes, serão realizadas as avaliações de adequabilidade dos controles existentes e de necessidade de criação de novos controles e, também, a contenção dos efeitos do incidente para as atividades.

4.7 Violações de Segurança

As violações das regras definidas nesta Política poderão ensejar a aplicação de medidas disciplinares, conforme determinam as normas de conduta do Código de Ética da Educredi.

4.8 Plano de Continuidade

Deve-se estabelecer, documentar, implantar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para os serviços e processos de negócios da Educredi, durante situações adversas.

4.9 Plano de Contingências

O Plano de Contingência da Cooperativa Educredi, estabelece os procedimentos a serem adotados pelos órgãos envolvidos direta ou indiretamente na resposta a emergências e desastres relacionados a eventos naturais ou invasão do servidor.

O presente Plano foi aprovado pelo Conselho de Administração e Diretoria Executiva, sendo nomeada a Coordenação juntamente com o Diretor Executivo para 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.

Tem como objetivo permitir a continuidade dos processos de negócios da Cooperativa Educredi afetada pela emergência, ameaça ou desastre tecnológico ou natural, além de assegurar a restauração das atividades, instalações e equipamentos o mais rápido possível e garantir a rápida ativação dos processos do negócio.

Na hipótese de qualquer incidente relevante e de interrupção de serviços relevantes, que configurem uma situação de crise, a Cooperativa informará ao Banco Central do Brasil e indicará quais serão as providências para o reinício das atividades. Ainda, na possibilidade de incidentes relevantes que possam ser passíveis de incidência em outras instituições financeiras, a Cooperativa se compromete a compartilhar as informações para auxiliar na prevenção de todas as instituições financeiras.

4.10 Gestão dos Prestadores de Serviços Relevantes

Devem ser estabelecidos e continuamente aprimorados os controles de segurança cibernética destinados a assegurar que as informações tratadas pelos seus fornecedores estejam devidamente protegidas.

4.11 Conscientização de Colaboradores, Associados, Terceiros e Fornecedores

Os recursos e as informações de propriedade ou sob custódia da Educredi devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas.

A política de segurança cibernética e da informação, normas e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos colaboradores, tanto pelas equipes de recursos humanos quanto pelos gestores.

Programas de conscientização, divulgação e reciclagem do conhecimento da política de segurança cibernética e da Informação devem ser estabelecidos e praticados regularmente para garantir que todos os colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

4.12 Exceções

Ocorrências relacionadas ao funcionamento da Política da Segurança Cibernética e da Informação, não contempladas neste regulamento, serão levadas para conhecimento e deliberação dos diretores e conselheiros de administração da cooperativa.

4.13 Penalidades

O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

4.14 Revisão e Atualização

A política de Segurança Cibernética e da Informação deverá ser revista e atualizada, ao menos anualmente, com vistas a se manter em sintonia com as regras de negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

5. RESPONSABILIDADES

Todo colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da cooperativa e deve cumprir as determinações da política, normas e padrões de segurança da informação.

5.1 Diretores e Conselheiros Administrativos

- Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;
- Prover comprometimento e apoio à aderência da política de segurança cibernética e da informação, de acordo com os objetivos e estratégias de negócio estabelecidas para organização;

- Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações;
- Fornecer à área de segurança da informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário.
- Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio.

5.2 Estagiários, Colaboradores e Terceiros/Prestadores de Serviços

- Cumprir as determinações da política, normas e procedimentos publicados pela Educredi;
- Orientar os funcionários da empresa sobre o cumprimento das determinações da política, normas e procedimentos publicados pela Educredi;
- Prestar os serviços de acordo com as tratativas em contrato;
- Cumprir com o acordo de confidencialidade.
- Notificar a área ou responsável de gestão de risco sobre as violações da política de segurança cibernética e da informação e sobre os incidentes de segurança que venha a tomar conhecimento;
- Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI.

5.3 Gestor

- Apoiar e incentivar o estabelecimento da política de segurança cibernética;
- Garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança da informação;
- Desenvolver, implantar, manter e aprimorar a segurança das informações;
- Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes, tomando os devidos cuidados para preservar a segregação de funções;
- Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos colaboradores que violarem o código de ética e conduta, a política de segurança cibernética e da informação e as normas da Cooperativa;
- Autorizar acessos de seus colaboradores apenas quando forem realmente necessários.

5.4 Conselho Fiscal e Auditoria

- Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
- Desenvolver e estabelecer programas de conscientização e divulgação da política de segurança cibernética e da informação;
- Conduzir o processo de gestão de riscos de segurança da informação;
- Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
- Propor projetos e iniciativas para melhoria do nível de segurança das informações.

5.5 Área de Infraestrutura

- Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;
- Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
- Conduzir a gestão dos acessos a sistemas e informações da Educredi;
- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
- Informar imediatamente a Diretoria, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da Cooperativa;
- Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;

6. EVENTOS ANALISADOS NO PLANO DE CONTINGÊNCIA

O plano de contingência foi elaborado visando vários tipos de eventos ou riscos operacionais externos, sendo os mais comuns:

1. Atos de Vandalismo;
2. Incêndios;
3. Ameaças de Bombas;
4. Roubos;
5. Interrupção do Fornecimento de Serviços Telecomunicação;
6. Interrupção do Fornecimento de Energia Elétrica;
7. Catástrofes Climáticas

O Plano de Contingência para Incêndios foi desenvolvido a partir da análise dos riscos identificados como possíveis pela Cooperativa.

a) CENÁRIOS DE RISCO

CENÁRIOS DE RISCO		
1.	NOME DO RISCO	Risco de Incêndio, Danos Elétricos, Roubo e/ou Furto, Risco de cataclismas climáticos e Explosão de Qualquer Natureza.
2.	LOCAL	Rua Getúlio Vargas, 283. Bairro Menino Deus – Porto Alegre
3.	DESCRIÇÃO	Sede Cooperativa Educredi
4.	FATORES CONTRIBUINTE	Sinistro
5.	RESULTADOS ESTIMADOS	Dano Parcial/Total de Material e Equipamentos de Trabalho dos Colaboradores da Cooperativa.

b) IDENTIFICAÇÃO DOS RISCOS

Os riscos identificados são:

1. Risco de Danos Elétricos;
2. Risco de Roubo e/ou Furto;
3. Risco de cataclismas climáticos;
4. Explosão de Qualquer Natureza.

c) CONTINGÊNCIAS DA INFRAESTRUTURA

I. Tecnológicas

- Estrutura disponibilizada:

Software de gerenciamento e controle de ativos da cooperativa.

Suas características são:

- Falhas, desempenho, serviços e auditoria da operação da gerência;
- Gerenciamento da operação baseado em serviços;
- Visualização gráfica do impacto que os eventos causam nos negócios;
- Detecção da causa raiz através da modelagem de serviços;
- Gerenciamento de performance e disponibilidade integradas;
- Gerenciamento do ambiente heterogêneo;
- Solução distribuída que monitora, controla e reporta a saúde do ambiente de TI;
- Visão única do ambiente gerenciado;
- Interface única;
- Gerenciamento de Falhas de Redes;
- Gerenciamento de ambientes;
- Interface web com uma visão dinâmica;
- Possibilidade de gerenciamento de eventos facilitando o conhecimento da causa raiz;
- Coleta de informações sobre a rede ajudando na identificação de problemas;
- Gerenciamento proativo;
- Acesso remoto via Web;
- Monitoração dos tempos de resposta dos caminhos da rede;
- Análise dos caminhos da rede baseado nas aplicações e protocolos;
- Diagnóstico e latência dos caminhos estáticos e dinâmicos da rede;
- Relatórios atuais e históricos com as informações dos caminhos da rede;
- Visualização gráfica dos caminhos da rede;
- Gerenciamento de Performance de Redes;
- Relatórios com informações para garantir a disponibilidade e máxima utilização dos recursos de rede;
- Relatórios técnicos / gerenciais com informações atuais;

II. Backup Lógico:

- A Cooperativa Educredi possui dois tipos de backups:
 - Backup realizado pela empresa Fácil Informática, através da 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;

- Os documentos da empresa estão na nuvem da Microsoft em caso de criptografia ou incêndio pasta pegar um computador e sincronizar os arquivos da nuvem ou restaurar versão anterior. O backup automático diário é realizado através do One Drive, com isso as informações estão disponíveis em nuvem com acesso em tempo real. Assim possibilita a restauração automática de até 30 dias atrás dos documentos na versão anterior e restaura da lixeira arquivos excluídos de até 30 dias. Realizado pela empresa PetróInfo, da qual é nossa terceirizada nos serviços de tecnologia a responsável, com sua sede da empresa em Porto Alegre.

d) SITUAÇÕES DE CONTINGÊNCIA PREVISTAS

I. Falha no Sistema de Telecom

- Responsável pela disponibilização dos serviços de internet e telefonia fixa, Empresas Vivo, Algar Telecom e Claro Empresas.
- Abrangência: Todos os colaboradores da cooperativa.
- Para as centrais telefônicas / telefonia fixa: A cooperativa de crédito faz uso de uma central telefônica que é a mesma da associação AGPTEA, quando ocorre algum problema nesta central, a responsabilidade de chamar algum técnico para constatar a falha é do pessoal da associação, a cooperativa não possui outras centrais e nem contato dos técnicos. Neste caso a cooperativa possui três telefones celulares de outra operadora para realizar e receber suas ligações.
- Procedimentos: Informar ao responsável da AGPTEA sobre a falha quando referente as centrais, entrar em contato com as empresas responsáveis pelos serviços prestados, verificando sempre a situação da região onde a cooperativa se encontra.
- Responsável: Coordenação da cooperativa, juntamente com a direção.

e) RESUMO DE CONTINGÊNCIAS E RESPONSÁVEIS

Contingência Operacional

Plano de Contingência Operacional	
Área Responsável:	Conselho de Administração, Diretoria Executiva e Coordenação.
Contatos de emergência na EDUCREDI	Elson Geraldo, Diretor e Vice-Presidente, e-mail: elsongsena@hotmail.com . Telefone: (51) 9.9907-5396 / (51) 9.9170-9447. Caroline Freitas Hernandez, coordenadora, e-mail: krolhernandez@hotmail.com , telefone (51) 9.9296-3030
Objetivo do Plano de Contingências:	Assegurar condições para continuidade no trabalho da cooperativa, quando ocorrer algum dano, acidente ou desastre natural, visando reduzir as perdas.

Contingência da área de TI:

Objetivo:	Dar seguridade ao banco de dados da cooperativa, tanto do sistema utilizado e suas atualizações, como de arquivos salvos no servidor.
Antes do Incidente:	Existem atualmente 2 backups sendo realizados, um pela empresa Fácil Informática, que o faz automaticamente e diariamente, e o outro empresa de TI PetroInfo, do qual possui backup disponível na Microsoft 365.
Durante o Incidente:	O acesso ao responsável pela empresa de TI é ágil, sendo o mesmo sempre está disponível para demandas. É realizada a comunicação do incidente.
Após a Contingência / Retorno à Normalidade	Deve ser verificado pelo responsável do TI um servidor para implantação do sistema fácil, para darmos retorno aos acessos.
Pessoa Responsável:	Marcio Petro Monticelli – Responsável pela empresa de TI, e-mail: marcio@petroinfores.com.br Telefone: (51) 9.8441-4406

f) MONITORAMENTO DO LOCAL

Atualmente o monitoramento do prédio é feito por câmeras e alarme, assim como conta com a empresa prestadora de serviços de segurança. Funcionário da Cooperativa 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 demais colaboradores presentes no local. Empresa monitora 24hs, sendo inserido na área de atendimento um botão de acionamento imediato a empresa de segurança.

g) ALARME

O prédio da Sede da Cooperativa Educredi possui Alarme de Incêndio, cujo monitoramento é realizado pela STV Segurança.

h) ACIONAMENTO DOS RECURSOS

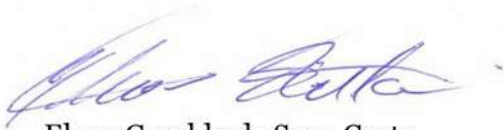
- A associação AGPTEA, responsável pelo prédio e espaço cedido a Cooperativa, possui um Contrato de Seguro com a Sompo Seguros, para toda a Sede Administrativa, (Apólice 1800615916).
- Atualmente a Cooperativa possui backup através do One Drive, que para restaurar deve selecionar uma data na lista suspensa e hora personalizada. Que deve ser preenchido os campos para ocorrer a restauração. Esta modalidade para ser realizada é necessário ter uma conta pessoal com uma assinatura Microsoft 365. Na qual fica aos cuidados da empresa TI PetroInfo.
- 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-14957-2020).

i) MOBILIZAÇÃO E DESLOCAMENTO DOS RECURSOS

- Mediante contato com a Sompo Seguros, será comunicado sinistro para que se tome as medidas providências.
- 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, site, telefones e em nossas redes sociais) sobre a ocorrência do sinistro e prazo para regularização.

j) RETORNO ÀS ATIVIDADES

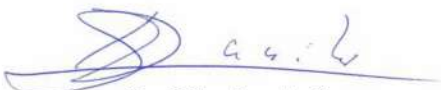
Após a regularização das condições da Sede, mediante contato com a seguradora, e disponibilização das instalações, serão restaurados backups de arquivos do sistema, possibilitando retorno às atividades da Sede da Cooperativa, sendo previsto o máximo de 5 dias úteis para volta das atividades.



Elson Geraldo de Sena Costa
Diretor Executivo



Gilberto Sidnei dos Santos
Diretor Administrativo



Danilo Oliveira de Souza
Presidente do Conselho de Administração