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 - I	30/2019	Aprovação	Caroline Hernandez
2020 – I. I	49/2020	Revisão e Implementação de acordo Resolução Bacen Nº 4.658	Caroline Hernandez

Sumário

1. OBJETIVO

A Política de Segurança Cibernética e da Informação é o documento que estabelece conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações da Cooperativa Educredi. Tem como objetivo definir os princípios fundamentais que formam a base da Política de Segurança Cibernética e da Informação, norteando a elaboração de normas, processos, padrões e procedimentos.

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, bem como a terceiros e prestadores de serviços, visando a abrangência de todos seus stakeholders.

3. CONCEITOS E DEFINIÇÕES

Recursos: qualquer ativo, tangível ou intangível, pertencentes a serviço ou sob responsabilidade da Educredi, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados em nuvem, sistemas e processos.

Ameaça: qualquer causa potencial de um incidente indesejado que possa resultar em impacto aos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

Boas Práticas de Segurança da Informação: são consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas.

Colaborador: entende-se como colaborador qualquer pessoa que trabalhe para a Cooperativa Educredi, quer seja: funcionário com registro em carteira de trabalho, terceiro, estagiário ou aprendiz.

Controle: qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança da informação. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas, padrões, software e outros.

Gestor: Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.

Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para a Educredi, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.

Princípios de "Least Privilege" e "Need do Know": estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know).

Política de Segurança Cibernética e da Informação: Conjunto de ações documentadas com as normas e padrões de segurança cibernética e segurança da informação a serem seguidos pela instituição.

Risco: qualquer evento que possa afetar a capacidade da cooperativa de atingir seus objetivos e sua estratégia de negócios.

Segurança da Informação (SI): é a proteção das informações, sendo caracterizada pela preservação de:

- Confidencialidade: garantia de que a informação somente será acessada por pessoas efetivamente autorizadas.

- Integridade: garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade.

- Disponibilidade: garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa.

- Conformidade: garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

Segurança Cibernética: conjunto de tecnologias, processos e práticas projetadas para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

Recursos Críticos: recursos essenciais para o funcionamento da operação da Cooperativa e que possuem informações críticas ou sensíveis.

Baselines: requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos.

Nuvem (Cloud): infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita.

IoT (Internet of Things – Internet das coisas): conexão de dispositivos eletrônicos, como aparelhos eletrodomésticos, eletro portáteis, máquinas industriais, meios de transporte, dentre outros utilizados no dia a dia à internet.

4. PAPÉIS e 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.

4.1 As responsabilidades da Alta Direção são:

I. Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;

II. 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;

III. Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações;

IV. Fornecer à área de segurança da informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário.

4.2 As responsabilidades dos Colaboradores são:

I. 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;

II. Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI.

4.3 As responsabilidades do Gestor são:

I. Apoiar e incentivar o estabelecimento da política de segurança cibernética;

II. Garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança da informação;

III. Desenvolver, implantar, manter e aprimorar a segurança das informações;

IV. Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes, tomando os devidos cuidados para preservar a segregação de funções;

VI. 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;

VII. Autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de need to know e least privilege.

4.4 As responsabilidades do Conselho Fiscal:

I. Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;

II. Desenvolver e estabelecer programas de conscientização e divulgação da política de segurança cibernética e da informação;

III. Conduzir o processo de gestão de riscos de segurança da informação;

IV. Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

V. Propor projetos e iniciativas para melhoria do nível de segurança das informações.

4.5 As responsabilidades da Área de Infraestrutura e Desenvolvimento

I. Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;

II. Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;

III. Conduzir a gestão dos acessos a sistemas e informações da Educredi;

IV. Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;

IV. Informar imediatamente a Diretoria, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da Cooperativa;

V. 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;

VI. Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio.

4.6 As responsabilidades da Área Jurídica são:

I. Apoiar a aplicação de medidas disciplinares referente a violações da política de segurança cibernética e da informação;

II. Identificar requisitos legais pertinentes à segurança da informação;

III. Garantir a adoção de cláusulas pertinentes à segurança das informações nos contratos estabelecidos com a cooperativa.

4.7 As responsabilidades de Fornecedores e Parceiros de Negócios são:

I. Cumprir as determinações da política, normas e procedimentos publicados pela Educredi;

II. Orientar os funcionários da empresa sobre o cumprimento das determinações da política, normas e procedimentos publicados pela Educredi;

III. Prestar os serviços de acordo com as tratativas em contrato;

IV. Cumprir com o acordo de confidencialidade.

4.8 Responsabilidades da Auditoria Interna

I. A efetividade dessa política, suas diretrizes e processos, assim como as devidas revisões e solicitações de atualizações caso necessário.

5. DIRETRIZES PARA TRATAMENTO DAS INFORMAÇÕES

- A informação deve ser utilizada de forma transparente e apenas para a finalidade para qual foi coletada;
- Todo processo de trabalho deve garantir a segregação de funções, por meio da participação de mais de um colaborador, para que a atividade não seja executada e controlada pelo mesmo colaborador;
- O acesso às informações e recursos devem estar de acordo com o porte da Cooperativa, e deve conter um Diretório para informações sigilosas;
- A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- A senha é utilizada como assinatura eletrônica e deve ser mantida de forma secreta;
- Toda informação que garanta a continuidade das atividades da Cooperativa, deverá ter cópia de segurança em local físico distinto, devidamente protegido para essa finalidade ou outro meio eficiente para permitir sua pronta recuperação em caso de perda ou danos;
- As informações contidas em material que se tornar disponível para descarte (papel, pen drives, cd etc.) deverão ser destruídas ou mantidas em locais fechados, protegidas do acesso de pessoas não autorizadas;
- Todo colaborador é responsável pela segurança da informação a que tem acesso;
- Toda informação encontrada extraviada deverá ser, imediatamente, devolvida a sua origem.

- Os colaboradores não devem efetuar tentativas de obter acesso às informações que não lhe são permitidos, devendo solicitá-las ao respectivo proprietário da informação, pasta ou arquivo;

- Qualquer processo de criação, processamento, armazenamento, transmissão e exclusão da informação devem ser protegidos e tratados individualmente (software, hardware, blindagens, autenticação e autorização);

- As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias nos seguintes níveis:

  I. Restrita;
  II. Confidencial;
  III. Interna;
  IV. Pública.

- As concessões, revisões e exclusões de acesso devem ser realizados através das ferramentas e processos da Cooperativa Educredi.

- Os riscos devem ser identificados pela empresa prestadora de serviços responsável pelo Setor de T.I, através de e-mail, sinalizando as vulnerabilidades e ameaças, sendo recomendadas as proteções adequadas.

- Os cenários de riscos devem ser discutidos em reunião do Conselho de Administração e Conselho Fiscal e aprovadas pela Diretoria da Cooperativa Educredi.

6. RECOMENDAÇÕES PARA USO DA INFORMAÇÃO/TECNOLOGIA

I. 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).

II. 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.

III. 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).

IV. Cada usuário é responsável pelo uso de recursos que de forma fisicamente são entregues e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados (ISO A.6.1.3).

7. RECOMENDAÇÕES PARA DO USO DO COMPUTADOR

I. O computador disponibilizado para o usuário é de propriedade da COOPERATIVA e tem por objetivo o desempenho das atividades profissionais desse usuário na organização;

II. É necessário que o Gestor do usuário o autorize a usar o computador, fazendo uma solicitação a Infraestrutura, que autorizará tecnicamente e fará a liberação mediante a disponibilidade de recursos;

III. Todos os equipamentos, softwares e permissões de acessos devem ser testados, homologados e autorizados pela área de infraestrutura para uso da Cooperativa;

IV. A Cooperativa pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário;

V. Os programas e aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura e TI;

VI. 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;

VII. A Cooperativa poderá verificar a qualquer momento, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pela área de infraestrutura;

VIII. 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;

IX. Todas as práticas que representam ameaças à segurança da informação serão tratadas com a aplicação de ações disciplinares;

X. O usuário é responsável por todo acesso realizado com a sua autenticação;

XI. 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;
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas raças ou gêneros.

XII. 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;

XIII. É proibido o uso de serviços de mensagem instantânea (MSN, whats app etc.) e pen drive através dos computadores da Cooperativa, exceto em eventuais situações de uso profissional autorizado pelo gestor;

XIV. 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;

XV. Periodicamente a área de infraestrutura poderá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Empresa;

XVI. É proibido o acesso aos serviços de correio eletrônico particular, tipo webmail, através dos recursos de tecnologia da Cooperativa Educredi, exceto em eventuais casos autorizados pelo Gestor;

XVII. A Cooperativa disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais (ex.: usuario@educredi.com.br);

XVIII. O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Cooperativa; passível de alterações de acordo com sua gestão;

XIX. 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;

XX. As caixas postais de contas de correio eletrônico da Cooperativa têm limite de tamanho de 3.2GB e as mensagens enviadas/recebidas poderão conter arquivos com até 20MB por mensagem;

XXI. O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da Cooperativa Educredi;

XXII. Em situações autorizadas pela Gerência, as mensagens do correio eletrônico de um usuário poderão ser acessadas pela Cooperativa ou por pessoas por ela indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal;

XXIII. 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, independentemente de serem legais ou ilegais; repassem propagandas ou mensagens de alerta sobre qualquer assunto.
- Havendo situações em que o usuário acredite ser benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos/Gerencia, que definirá a sua publicação ou não.

XXIV. Proibido ainda, mensagens que 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 Educredi; sejam incoerentes com o Código de Ética.

XXV. 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.

8. RECOMENDAÇÃO AO USO DO TELEFONE

I. A Cooperativa Educredi disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais;

II. Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela Gestão e Diretoria Executiva;

III. O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade da Cooperativa;

IV. 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.

9. CONTROLE DE ACESSO A COMPUTADORES E REDE

- O acesso às estações de trabalho de forma remota só deverá ocorrer mediante autorização do gestor e usuário da estação de trabalho, e para isso, o setor de infraestrutura deverá instalar o programa, proporcionando assim o acesso remoto seguro;

- É de responsabilidade da cooperativa qualquer acesso remoto, que seja efetuado por terceiros utilizando programas não licenciados e/ou não autorizados.

10. PRECAUÇÕES DOS EQUIPAMENTOS QUE ARMAZENAM DADOS E INFORMAÇÕES

- Quando os equipamentos que armazenam dados e informações forem vendidos, devolvidos ao fabricante, enviados para manutenção ou doados para instituições e outras finalidades do tipo, as informações neles contidas devem ser destruídas antes de deixar as dependências da Cooperativa Educredi.

11. LICENCIAMENTO DE SOFTWARES

I. Todo equipamento deverá ter o seu sistema operacional devidamente licenciado, obedecendo os termos de utilização do fabricante;

II. Softwares de uso diário, que não possuírem licenças gratuitas, também deverão obedecer às regras de licenciamento do fabricante;

III. O setor de Infraestrutura não tem autorização para efetuar instalações de softwares não licenciados. Se a cooperativa optar pela instalação de um software não licenciado, a mesma se responsabilizará pelas penalidades/multas que tal ação poderá acarretar.

12. DIRETRIZES PARA SEGURANÇA FÍSICA DE COMPUTADORES

I. Todos os equipamentos que armazenam informações e dados, que são essenciais para o funcionamento da cooperativa, deverão estar armazenados em locais devidamente protegidos contra o acesso de pessoas não autorizadas;

II. Os equipamentos não ligados à rede (micros "standby") e que armazenam informações de alto e médio risco, deverão estar instalados em locais que garantam a segurança física desses equipamentos, incluindo sistemas que mantenham o fornecimento de energia elétrica, climatização e a recuperação dos dados caso haja necessidade de utilizar esse equipamento em algum momento;

III. Os equipamentos como notebooks, computadores e servidores que estejam ligados a uma rede, deverão manter as informações classificadas como de alto e médio risco no servidor;

IV. Todas as pessoas que estiverem autorizadas a utilizar informações da Educredi fora de suas dependências físicas, deverão obedecer às mesmas diretrizes estabelecidas para os equipamentos instalados internamente;

V. A cooperativa poderá indicar um funcionário, além da Gestora para ter um administrador local, treinado pela área de TI (empresa terceira da Cooperativa), que terá autonomia para executar tarefas e procedimentos, contanto que cumpra os itens desta resolução e as Normas estipuladas.

13. SERVIDOR

- O servidor deverá estar instalado em uma estrutura que garanta a segurança física, incluindo climatização, sistemas que mantenham fornecimento de energia elétrica estabilizada e recuperação de dados.

14. CONSCIENTIZAÇÃO E DIVULGAÇÃO DA SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

- 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.

15. INCIDENTES DE SEG. DA INFORMAÇÃO

I. São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de SI: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio em risco.

II. Violações ou tentativas de violação desta política, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

III. Colaboradores devem informar imediatamente à segurança da informação todas as violações à política de segurança da informação, normas, padrões incidentes ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

IV. A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos até que sejam concluídas as investigações necessárias.

16. SEGURANÇA EM REDES

- Devem existir controles tecnológicos para proteger o acesso entre redes (incluindo Internet, redes públicas, extranets, acesso remoto, wireless e as diferentes redes de usuários).

- O acesso remoto somente será permitido para Gestores e/ou situações em que for indispensável.

- Os níveis de segurança (confidencialidade, integridade e disponibilidade) esperados dos serviços de comunicações, devem ser estabelecidos nos contratos firmados com os fornecedores desses serviços.

17. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

- Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

18. SERVIÇOS DE NUVEM

I. Toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicado ao Banco Central do Brasil, via siscom ou protocolo digital da autarquia.

II. Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados devem possuir acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados.

III. 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.

IV. 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.

V. 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.

VI. 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.

19. EXCEÇÕES

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

20. 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.

21. 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.

22. DAS REFERÊNCIAS

Para um entendimento mais abrangente sobre a política de Segurança Cibernética e da Informação, deve-se consultar os documentos abaixo referenciados:

- Resolução Nº 4.658, DE 26 DE ABRIL DE 2018.

23. DAS DÚVIDAS

Em caso de dúvidas deve-se solicitar esclarecimentos a diretoria executiva da cooperativa juntamente com sua gestão.

24. CONTINUIDADE DE NEGÓCIO

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.

25. 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.

25.1 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. Inundações;

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

25.2. CENÁRIOS DE RISCO

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

25.3. IDENTIFICAÇÃO DOS RISCOS

Os riscos identificados são:

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

26. CONTINGÊNCIAS DA INFRAESTRUTURA

I. Tecnológicas

- Estrutura disponibilizada:

Software de gerenciamento e controle de ativos da cooperativa. Suas características são:

- Gerenciamento de Servidores;
- 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 três tipos de backups:

  - Backup realizado pela empresa Fácil Informática, empresa que nos fornece o software do atendimento e processos. Este backup é realizado diariamente e automaticamente, caso ele não se realize por algum motivo, todos os funcionários recebem uma mensagem ao tentar acessar o programa, comunicando que é necessário o backup manual. Todos os funcionários estão aptos a realizarem o backup manual, é um processo simples.

- O backup realizado pelo HD externo, segundo informações do responsável pela TI, este backup também é realizado diariamente, salvando todos os dados dos programas e arquivos.

- O terceiro backup é o realizado diretamente pela empresa Pétro Info, da qual é nossa terceirizada nos serviços de tecnologia e possui um servidor com as informações em sua sede da empresa em Porto Alegre.

26.1 SITUAÇÕES DE CONTINGÊNCIA PREVISTAS:

I. Falha no Servidor

a) Abrangência: Todos os funcionários da cooperativa.
b) Contingências Existentes: Contatar o TI terceirizado para disponibilização de um novo servidor e caso necessário a utilização do que consta em sua empresa física. Atualmente a cooperativa de crédito possui apenas um servidor em sua unidade em Porto Alegre.
c) Procedimento: Entrar em contato com a empresa PetroInfo, responsável pela TI.
d) Responsável: Coordenador da cooperativa.
e) A equipe de TI colocará no ar o servidor que apresentou falha, realizando todos os testes necessários no ambiente de produção.

II. Falha no Sistema de Telecom

a) Responsável pela disponibilização dos serviços de internet e telefonia fixa, Empresa Algar Telecom e Claro Empresas.
b) Abrangência: Todos os colaboradores da cooperativa.
c) 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.

d) 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.

e) Responsável: Coordenação da cooperativa, juntamente com a direção.

27. 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 três backups sendo realizados, um pela empresa Fácil Informática, que o faz automaticamente e diariamente, os outros dois são pela empresa de TI PetroInfo, da qual possui um backup em um HD externo e outro backup em sua sede, em Porto Alegre.
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@petroinforedes.com.br Telefone: (51) 9.8441-4406

28. 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.

29. ALARME

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

30. ACIONAMENTO DOS RECURSOS

I. 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).

II. Atualmente a Cooperativa possui sua base de dados composta por Backups. Um desses Backups (Sistema e Arquivos Internos da Cooperativa) fica aos cuidados de uma empresa que presta os serviços de T.I, no qual ficam armazenados em um servidor externo, localizado em sua sede. Esses mesmos arquivos ficam aos cuidados da Gerente da Cooperativa Educredi, que diariamente o retira das dependências (HD externo). Em sua ausência fica funcionário definido pela gestora os cuidados do HD externo.

III. 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).

31. MOBILIZAÇÃO E DESLOCAMENTO DOS RECURSOS

I. Mediante contato com a Sompo Seguros, será comunicado sinistro para que se tome as medidas providências.

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

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

32. 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 Presidente Executivo

ERNI JOSE DA SILVA
Diretor Presidente Administrativo