PRIMACREDI
CrediSIS

Política Institucional de Segurança da Informação e Segurança Cibernética

CONTROLE DE VERSÕES

VERSÃO	ORDEM	DESCRIÇÃO	AUTOR	APROVAÇÃO CONSAD
1.0	1	Criação do Documento	DIREX	Ata 10/2012 - 18/10/2012
2.0	2	1ª Revisão	DIREX/UCI	Ata 12/2016 - 16/12/2016
2.1	3	Revisão	TI/UCI	Ata 06/2019 - 25/04/2019
2.2	4	Atualização	TI/UCI	Ata 15/2020 - 26/11/2020
3.0	5	Revisão e atualização	TI/UCI	Ata 17/2022 - 27/10/2022

LEGENDA	
CONSAD	*Conselho de Administração*
DIREX	*Diretoria Executiva*
UCI	*Unidade de Controle Interno*
TI	*Tecnologia da Informação*

DIREX ADM	DIREX NEG	DIREX FIN

SUMÁRIO

DIREX ADM	DIREX NEG	DIREX FIN

1. DO OBJETIVO

A **Política Institucional de Segurança da Informação e Segurança Cibernética** tem por objetivo estabelecer diretrizes e normas que permitam aos colaboradores da PRIMACREDI seguirem padrões de comportamento adequados às necessidades do negócio, da proteção legal e do indivíduo no tocante à segurança da informação e segurança cibernética, além de nortear a definição de procedimentos específicos e a implementação de controles e processos para o seu atendimento afim de garantir a continuidade dos negócios da empresa frente a ameaças .

Visa prover diretrizes para a segurança da informação e segurança cibernética, relacionadas ao manuseio, controle, proteção (contra indisponibilidade, divulgação imprópria, acesso indevido e modificação não autorizada de informações e de dados) e descarte, bem como, zelar pelo dever de sigilo das operações de instituições financeiras conforme Lei Complementar n° 105/01, e a observância à Resolução n° 4.658/18 - CMN e suas disposições futuras.

2. DOS CONCEITOS E SIGLAS

Para fins desta Política são observados os seguintes conceitos:

Informação: Dados ou conjunto de dados que possuam algum propósito e valor para o CrediSIS, 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.

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

DIREX ADM	DIREX NEG	DIREX FIN

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 das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

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

I. **Confidencialidade**: garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;

II. **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;

III. **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;

Segurança Cibernética: Conjunto de tecnologias, processos e práticas, projetados para proteger redes, computadores, sistemas e dados, de ataques, danos, acidentais ou não, e acessos não autorizados, visando proteger somente assuntos relacionados ao digital.

Malware: termo que se refere a softwares/códigos maliciosos utilizados para infectar dispositivos ou sistemas com intuito de causar danos, alterações, roubo de informações, entre outros. São exemplos de malware, vírus, trojan e worm.

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 irrestrita.

DIREX ADM	DIREX NEG	DIREX FIN

IDS e IPS: Acrônimos de Intrusion Detection System e Intrusion Prevention System, são sistemas de detecção e prevenção a intrusão, a Finalidade do IDS é identificar atividades anômalas na infraestrutura de redes ou de dispositivos, já o IPS que é um Complemento não obrigatório aos IDS, tem por finalidade a execução automática de ações já previstas nas políticas do sistema ou em outras bases de referência internas e/ou externas.

Storages: é um hardware que contém slots para vários discos em redundância, capaz de armazenar dados da instituição, ligado aos servidores através de ISCSI ou fibra óptica.

Malware: termo que se refere a softwares/códigos maliciosos utilizados para infectar dispositivos ou sistemas com intuito de causar danos, alterações, roubo de informações, entre outros. São exemplos de malware, vírus, trojan e worm.

Backup - Cópia de Segurança

3. DOS PRINCÍPIOS

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso da Cooperativa. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos à PRIMACREDI e prejudicar o crescimento e as vantagens competitivas. Atentos a isso, a **Política Institucional de Segurança da Informação e Segurança Cibernética** é o alicerce dos esforços de proteção às informações da PRIMACREDI.

DIREX ADM	DIREX NEG	DIREX FIN

Segurança da Informação são esforços contínuos para a proteção dos ativos de informações, auxiliando os administradores a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

Disponibilidade: garantir que as informações estejam disponíveis à todas as pessoas autorizadas a tratá-las.

4. DA REGULAMENTAÇÃO

I. ISO 27001 - Norma que define a organização da segurança da informação em qualquer tipo de empresa, é também uma certificação;

II. Resolução CMN nº 4.893/2021 – Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;

III. Circular Bacen nº 3.909 – Segurança Cibernética.

5. DAS RESPONSABILIDADES E ATRIBUIÇÕES

Esta **Política Institucional de Segurança da Informação e Segurança Cibernética** da PRIMACREDI:

DIREX ADM	DIREX NEG	DIREX FIN

5.1. Responsabilidades da Alta Direção

I. Garantir aderência à Política de Segurança da Informação e Segurança Cibernética de acordo com os objetivos e estratégias de negócio estabelecidas pela Primacredi.

II. Seguir e aplicar as diretrizes de segurança previstas nos normativos da Primacredi.

III. Definir os níveis de risco aceitáveis.

5.2. Responsabilidades do Colaborador

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

II. Notificar a área de Gestão de Risco e ao Gestor sobre as violações da Política de Segurança da Informação e sobre os incidentes de segurança que venha a tomar conhecimento.

5.3. Responsabilidades do Gestor/Coordenador

I. Apoiar e incentivar o estabelecimento da Política de Segurança da Informação e Segurança Cibernética.

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

III. Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos colaboradores que violarem o Código de Ética e Conduta, a Política de Segurança da Informação e as normas da PRIMACREDI;

IV. Autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de Necessário saber e Privilégio mínimo;

DIREX ADM	DIREX NEG	DIREX FIN

V. Definir o valor da informação e dos ativos de informação sob sua responsabilidade, baseando-se no valor que este representa para o negócio.

5.4. Responsabilidades da Área de Gestão de Risco

I. Conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

III. Supervisionar a resolução e o tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;

IV. Mapear os riscos de segurança da informação, em conjunto com as áreas, apoiando nos planos de ação e medidas para resolução ou mitigação dos riscos.

V. IV. Definir mecanismos para acompanhamento e controle que assegurem a implementação da política de segurança da informação.

VI. V. Aplicar e supervisionar a aplicação das premissas de segurança conforme estabelece o Regimento Interno da cooperativa, Políticas Específicas, Manual do Colaborador, Código de Ética e Conduta, Regimento Interno e Manual Operacional;

Parágrafo único: Fica o Controle Interno responsável por monitorar e acompanhar os planos de ações que visam regularizar as inconformidades detectadas nos relatórios de monitoramento acerca do cumprimento da presente política, os quais serão elaborados mensalmente. O acompanhamento será realizado por meio de sistema automatizado, seguindo o mesmo fluxo descrito na Política de Supervisão.

DIREX ADM	DIREX NEG	DIREX FIN

5.5. Responsabilidades da Área de Infraestrutura de TI

I. Gerir adequadamente os ativos e acessos de infraestrutura de TI, sejam eles internos ou em nuvem.

II. Orientar e coordenar as ações de segurança cibernética necessárias para a Central e cooperativas filiadas.

III. Manter atualizada, a infraestrutura tecnológica, de acordo com as melhores práticas e recomendações de mercado no que se refere a hardwares e softwares.

IV. Conduzir o processo de análise de vulnerabilidades, tratar os identificados em ativos, sistemas ou processos sob sua responsabilidade e acompanhar o andamento para saneamento das vulnerabilidades na área de Sistemas.

V. Tratar os riscos identificados através de mapeamento, em conjunto com a área de riscos.

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

VII. Informar imediatamente a área de Gestão de Riscos, sobre violações, falhas,

VIII. anomalias e outras condições que possam colocar em risco as informações e ativos de TI da CrediSIS.

IX. 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.

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

XI. Garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como Data Centers. Estes

DIREX ADM	DIREX NEG	DIREX FIN

devem conter controles adequados e todas as proteções e contingências necessárias para a sua respectiva proteção.

XII. Apoiar a área de gestão de riscos para garantir o cumprimento da política de segurança da informação.

5.6. Responsabilidades de Fornecedores e Parceiros de Negócio

I. Cumprir as determinações da Política, Normas e Procedimentos publicados pela Central CrediSIS e suas singulares;

II. Orientar seus funcionários sobre o cumprimento das determinações desta Política, Normas e Procedimentos publicados pela Central CrediSIS e suas singulares;

III. Cumprir com o NDA (Non Disclosure Agreement) do CrediSIS.

5.7. Responsabilidades da Área de Gestão de Pessoas

I. Cumprir com o processo formal de avaliação dos candidatos a emprego, de acordo com a ética, leis e normativos vigentes, em especial a política de recrutamento e seleção da CrediSIS.

II. Garantir que a Política, Normas e Procedimentos desta política sejam divulgados no processo de admissão/integração de novos Colaboradores.

III. Desenvolver e estabelecer programas de conscientização e divulgação contínua desta política.

IV Informar às áreas sobre afastamentos, férias ou demissão de colaboradores para revogação dos acessos.

DIREX ADM	DIREX NEG	DIREX FIN

6. PRINCÍPIOS E DIRETRIZES

1. As diretrizes estabelecidas nesta **Política Institucional de Segurança da Informação e Segurança Cibernética**, deverão ser aplicadas em toda a Cooperativa e em qualquer local onde se encontrem ativos de informação da PRIMACREDI, que devem ser seguidos por todos os colaboradores internos, externos e parceiros, devendo ser aplicados em qualquer meio ou suporte;
2. A Cooperativa adota regras e soluções que protegem a segurança da rede de dados e de todos seus ativos de Tecnologia de Informação, para garantia da confidencialidade, do sigilo e da integridade das informações;
3. A todos os ativos de informação são aplicados requisitos de classificação de acordo com regras institucionalizadas definidas com base nos aspectos legais e necessidades do negócio;
4. Todos os equipamentos informatizados e de comunicação, sistemas e informações deverão ser utilizados pelos colaboradores internos e externos para realização de atividades exclusivamente profissionais;
5. Todo o acesso às informações e a utilização dos recursos corporativos poderão ser monitorados, não sendo permitido ao usuário o uso destes para atividades que não estejam relacionadas ao exercício das suas atividades;
6. Qualquer acesso às informações da Cooperativa será previamente autorizado pela área competente, levando em conta estritamente as atividades desenvolvidas pelo usuário dentro da Cooperativa. Quando por meio de sistema, o acesso só será permitido a usuários devidamente cadastrados e autorizados;

DIREX ADM	DIREX NEG	DIREX FIN

7. O acesso remoto, tanto interno quanto externo, deverá ser efetuado utilizando tecnologias adequadas e aprovadas para tal finalidade, respeitando os limites de supervisão, políticas e termos de responsabilidade estabelecidos.

8. As senhas de acesso são individuais, intransferíveis, de responsabilidade única e exclusiva do usuário e não podem ser compartilhadas ou divulgadas. As senhas respeitarão regras de complexidade mínima definidas pela Cooperativa;

9. Os acessos dos usuários à rede e aos sistemas serão revisados e atualizados, no mínimo, semestralmente;

10. Todo e qualquer dispositivo de identificação pessoal, não poderá ser compartilhado com outras pessoas, em nenhuma hipótese, sendo o colaborador, ainda que externo, responsável pelo uso correto de suas informações de identificação perante a Cooperativa e perante a legislação;

11. Na admissão ou transferência de colaborador de um setor para outro o Departamento de Recursos Humanos deverá comunicar ao Departamento de Tecnologia de Informação, tempestivamente, a criação ou adequação do usuário, já com as definições de perfil ao qual o mesmo deverá executar em suas atividades conforme as atribuições definidas pelo Gestor do novo Departamento;

12. Todos os acessos devem ser imediatamente bloqueados (tornarem-se inativos), assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar ao Departamento de Tecnologia de Informação, a fim de que o acesso seja bloqueado imediatamente. O login do usuário será mantido por no mínimo seis meses para fins de prevenção à fraude;

13. Os acessos em ausências, férias, licenças e atestados deverão ser adotados procedimentos internos específicos, estando na responsabilidade do

DIREX ADM	DIREX NEG	DIREX FIN

Departamento de Recursos Humanos a comunicação ao Departamento de Tecnologia de Informação;

14. Cabe aos Gestores dos Departamentos da PRIMACREDI a responsabilidade pela manutenção, revisão e cancelamento de autorizações de acessos a determinada informação ou conjunto de informações pertencentes a Cooperativa ou sob sua guarda, cabendo a ele o compromisso de informar ao Departamento de Recursos Humanos as alterações necessárias;

15. O uso do correio eletrônico da Cooperativa é para fins corporativos e relacionados às atividades do colaborador dentro da PRIMACREDI, não sendo permitido o uso para fins pessoais. Portanto, por medidas de segurança e manutenção das políticas internas, a organização tem o direito de monitorar as caixas de e-mails de todo o quadro de pessoal. A Cooperativa poderá tomar as medidas judiciais cabíveis para impedir o envio de mensagens com conteúdo ilegal ou spams. É proibida a criação de contas de correio eletrônico corporativo para terceiros que tenham ou não serviços vinculados à Cooperativa;

16. Não poderá ocorrer redirecionamento do correio eletrônico do colaborador, sendo de responsabilidade do mesmo o acesso as informações de caráter individual, nas ausências o colaborador deverá cadastrar uma mensagem de resposta com a informação de seu substituto e o e-mail;

17. As senhas devem ser criadas com expiração imediata, forçando a sua alteração pelo usuário no primeiro acesso, os usuários deverão criar senha com no mínimo 6 caracteres obedecendo a complexidade mínima exigida pelos sistemas. Caso o colaborador esqueça sua senha deverá requisitar via e-mail ou comparecer ao Departamento de Tecnologia de Informação para solicitar a troca ou cadastrar nova senha;

DIREX ADM	DIREX NEG	DIREX FIN

18. Cabe à PRIMACREDI definir as regras para a guarda e preservação das informações da Cooperativa, conforme o nível de classificação, sendo de responsabilidade do proprietário da informação armazená-la conforme as regras institucionalizadas para cópias de segurança (backup);

19. Documentos imprescindíveis para as atividades dos colaboradores deverão ser salvos em drives de rede. Os arquivos gravados apenas localmente nos computadores (por exemplo C:), não terão garantia de backup e poderão ser perdidos, caso ocorra uma falha no computador, furto ou qualquer sinistro, e assim acontecendo o usuário poderá ser responsável por negligência;

20. Os equipamentos, a tecnologia e os serviços fornecidos para o acesso à internet são de propriedade da Cooperativa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede ou na internet. Toda informação que é acessada, transmitida, recebida ou produzida na internet está sujeita à auditoria, portanto, a Cooperativa, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos à internet. Como regra geral, não poderá ser exposto, armazenado, distribuído, editado, impresso ou gravado, por meio de qualquer recurso, materiais de caráter abusivo, difamatório e de qualquer natureza sexualmente explícita;

21. As informações produzidas no ambiente da Cooperativa, por meio de seus recursos ou na execução de serviço contratado são de propriedade da Cooperativa e só poderão ser copiadas, divulgadas, publicadas, com autorização da área competente;

22. Informações confidenciais não serão discutidas em locais públicos ou com circulação de pessoas não ligadas a Cooperativa;

DIREX ADM	DIREX NEG	DIREX FIN

23. As instalações que abrigam informações, documentos e equipamentos de processamento de informação sensível são armazenadas em perímetros de segurança com controles apropriados que garantam o acesso apenas a pessoas autorizadas e possuem mecanismos de prevenção a incêndios e outros tipos de sinistros;

24. O Departamento de Tecnologia de Informação deve configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores em geral, com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta **Política Institucional de Segurança da Informação e Segurança Cibernética**, **Política Operacional de Segurança da Informação** e no Plano de Contingência da área de Tecnologia da Informação, disposto no **Plano de Continuidade do Negócio** da PRIMACREDI;

25. Todos os softwares utilizados na gestão da Cooperativa são licenciados. Não são instalados, conectados e utilizados softwares não autorizados pela área responsável, independente da natureza de uso ou aplicação. A entidade e os usuários respeitam o direito à propriedade intelectual, de acordo com a legislação em vigor, não reproduzindo ou divulgando material sem a autorização de seu autor;

26. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos e os colaboradores não poderão, em hipótese alguma, utilizar os recursos da PRIMACREDI para fazer o download ou a distribuição de software ou dados “pirateados”, atividade considerada delituosa, de acordo com a legislação nacional;

DIREX ADM	DIREX NEG	DIREX FIN

27. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação realizada nos equipamentos, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de Tecnologia de Informação ou de quem o setor determinar;

28. É vedada a instalação, conexão ou utilização de quaisquer dispositivos de armazenamento e conectividade (modem de rede de dados móvel, HD externo, flash-drive, pen-drive, etc.), salvo os de propriedade da PRIMACREDI ou autorizados pelo Departamento de Tecnologia de Informação.

29. Arquivos pessoais ou não pertinentes ao negócio da PRIMACREDI (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, em hipótese alguma. Quando identificada a existência de arquivos pessoais, o Departamento de Tecnologia de Informação comunicará o responsável direto, oferecendo prazo para remoção. Não tomadas as devidas providências, o Departamento de Tecnologia de Informação poderá eliminar os arquivos diretamente do local onde se encontram;

30. Para os contratos firmados com terceiros, a Cooperativa inclui cláusulas de confidencialidade, de acordo com o nível de serviço e em cumprimento a todas as regras definidas nesta Política e aos documentos a ela subordinados;

31. A Cooperativa se exime de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direto de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios;

32. Os riscos de segurança da informação devem ser devidamente gerenciados, de maneira integrada aos demais riscos inerentes às atividades da cooperativa.

33. A Cooperativa mantém o Plano de Resposta a Incidentes seguindo as diretrizes da Política de Gestão de Incidentes de Segurança da Informação.

DIREX ADM	DIREX NEG	DIREX FIN

34. Para adoção de regime home office a Cooperativa segue as diretrizes e recomendações de segurança descritas nesta política.

35. A Cooperativa mantém mecanismos de detecção e prevenção a intrusão aptos a mitigar riscos que possam impactar as atividades do sistema.

36. A Cooperativa mantém controles antimalware, individuais e atualizados, aptos a proteger os dispositivos que possam acessar informações corporativas do CrediSIS.

37. É de inteira responsabilidade de cada colaborador, qualquer prejuízo ou dano que sofrer ou causar a Cooperativa e/ou a terceiros, em decorrência da não obediência às diretrizes e normas internas;

38. A Cooperativa aplica penalidades nos casos de infrações às regras desta Política e documentos a ela subordinados, de acordo com o grau de impacto da infração;

39. As normas legais prevalecem sobre esta Política, sempre que houver divergência ou conflito.

7. PLANO DE CONTINGÊNCIA E ARMAZENAMENTO EM NUVEM

Disposto no **Plano de Continuidade do Negócio** da PRIMACREDI, o Plano de Contingência, apresenta a estratégia adotada no desenvolvimento da infraestrutura de Tecnologia da Informação da PRIMACREDI, de forma a ter alta disponibilidade e condições para uma rápida resposta a catástrofes que impeçam o acesso as dependências da Cooperativa ou restauração do ambiente de produção em caso de acidente crítico, assim como, os dispositivos de segurança adotados pela PRIMACREDI, na prevenção a ataques cibernéticos e como proceder caso um ataque seja bem sucedido.

DIREX ADM	DIREX NEG	DIREX FIN

A PRIMACREDI não possui contratos com empresas terceiras para armazenamento e processamento em nuvem para dados e sistemas próprios. Para soluções terceiras que venham a agregar serviços prestados, são exigidos em contrato, redundância para todos os itens de tecnologia envolvidos, além de que, os terceiros envolvidos devem estar em compliance com normas e resoluções vigentes no país e órgãos reguladores para instituições financeiras.

A PRIMACREDI poderá utilizar serviços de computação e armazenamento em nuvem, considerando o teor das informações. Qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada ao Banco Central do Brasil.

8. COMUNICAÇÃO E COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES

A política de gestão de incidentes de segurança da informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes da segurança da informação da PRIMACREDI e visa orientar o funcionamento do processo de gestão de incidentes de segurança cibernética e da informação, de forma que estes sejam tratados adequadamente, reduzindo ao máximo os impactos para os negócios.

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

DIREX ADM	DIREX NEG	DIREX FIN

A Primacredi possui ferramentas de proteção para minimizar a ocorrência de incidentes relevantes, mas, caso ocorra um incidente, primeiramente ele será analisado e comunicado a alta administração da PRIMACREDI (Conselho de Administração e Diretoria Executiva) e aos responsáveis pelas áreas mais impactadas pelo incidente, através de registros e após essa análise, é elaborado um plano de ação para corrigir e melhorar o processo, com o objetivo de cessar a incidência de novas ocorrências da mesma natureza. A elaboração e acompanhamento do plano de ação são coordenados pelo Departamento de Tecnologia da Informação em conjunto com a área de riscos, apresentado ao Conselho Fiscal, Diretor responsável e demais envolvidos no processo em que ocorreu o incidente.

9. DISPOSIÇÕES GERAIS

Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a Segurança da Informação e Segurança Cibernética, no âmbito da Cooperativa.

A revisão desta Política deve ocorrer a cada 1 (um) ano, ou a qualquer tempo conforme necessidade interna e/ou alteração regulatória.

DIREX ADM	DIREX NEG	DIREX FIN

10. VIGÊNCIA

A Revisão desta política foi aprovada pela Diretoria Executiva, conforme emissão da Minuta de Resolução Interna Nr.439.27.10/2022 encaminhada para apreciação do Conselho de Administração e divulgada pela Diretoria Executiva pela Resolução Interna Nr.448.29.10/2022.

A revisão desta Política foi homologada em reunião do Conselho de Administração, Ata 17/2022 no dia 27 de outubro de 2022, passando a vigorar a partir desta data.

Primavera do Leste/MT, 27 de outubro de 2022.

Diretoria Executiva:

Laura Beatriz Gomes da Mota Costa
CPF nº424.618.471-34
Diretora Administrativa

Benhur Alvarenga Ravanello
CPF nº017.437.201-90
Diretor de Negócios

Sebastião Filho Correa Vilela
CPF nº650.736.491-68
Diretor Financeiro