Uniprime cooperativa de crédito	**POLÍTICA DE SEGURANÇA CIBERNÉTICA**		
Elaborado por: Uniprime Central Nacional – Área de Gerenciamento de Riscos e Conformidade			Data da Criação: 18/04/2016
Aprovador por: Conselho de Administração		Ata n.º 269	Data Aprovação: 29/05/2026
Início da vigência: 18/04/2016	Revisado em: 27/05/2026		

Sumário

1 OBJETIVO

A Política de Segurança Cibernética do Sistema Uniprime tem como objetivo garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas de informação utilizados pela Cooperativa, protegendo as informações e transações dos cooperados, o sigilo das operações e a continuidade dos negócios, em conformidade com a regulamentação vigente.

A Política estabelece medidas baseadas em risco para prevenir, detectar, tratar e responder a incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, mitigando riscos cibernéticos, protegendo processos críticos e promovendo a melhoria contínua da segurança da informação.

2 REFERÊNCIAS NORMATIVAS

Esta Política observa a legislação e regulamentação vigentes, normativos internos aplicáveis, incluindo, mas não se limitando a:

- Plano de Ação e de Respostas a Incidentes de Segurança Cibernética;
- Plano de Continuidade de Negócios;
- Procedimento para Enquadramento de Fornecedor;
- Resolução CMN nº 4.893/2021;
- Resolução CMN 5274/2025;
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD);
- Lei Complementar nº 105/2001;
- Resolução CMN nº 4.557/2017.

3 ABRANGÊNCIA

A presente Política aplica-se ao Sistema Uniprime e deverá ser observada por Colaboradores, membros da alta administração e Conselho de Administração,

prestadores de serviços, fornecedores e demais terceiros que atuem em processos, sistemas, ambientes ou serviços relacionados às atividades do Sistema Uniprime, incluindo Fornecedores Relevantes.

4 DEFINIÇÕES

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como, a possibilidade de usar os ativos de informação da instituição.

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

Ativos de Tecnologia: são todos os recursos tecnológicos pertencentes, utilizados ou gerenciados pela organização que suportam suas operações e o tratamento de informações. Incluem, mas não se limitam a hardware (computadores, servidores, dispositivos móveis), software (aplicações, sistemas operacionais), redes, bancos de dados, serviços em nuvem e quaisquer outros componentes tecnológicos.

Autenticação: processo de verificação da identidade de um usuário ou sistema como: senha, biometria, MFA.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Backup: cópia de segurança de dados armazenada para recuperação em caso de perda, falha ou incidente.

Colaboradores: conjunto de pessoas que atuam em nome do Sistema Uniprime, incluindo empregados, membros da diretoria, estagiários, jovens aprendizes, prestadores de serviços e quaisquer outros prepostos.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada.

Conformidade em Segurança da Informação: cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação da organização.

Continuidade de Negócios: capacidade estratégica e tática de o Sistema Uniprime planejar e responder a incidentes e interrupções de negócios, minimizando impactos operacionais, financeiros, regulatórios e reputacionais, até a plena normalização das atividades.

Criptografia: prática de proteger informações por meio da conversão de dados em algoritmos codificados, acessível apenas por quem possui a chave de decriptação.

Data Loss Prevention (DLP): Solução de Prevenção contra Perda de Dados, que consiste em um conjunto de ferramentas e processos utilizados para garantir que dados sensíveis não sejam perdidos, mal utilizados ou acessados por usuários não autorizados. Atua na detecção e prevenção de vazamentos e violações de dados.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade.

Fornecedor Relevante: fornecedor ou prestador de serviços, cuja relação comercial possa impactar significativamente a continuidade operacional, a conformidade regulatória, a segurança da informação, a situação financeira, a reputação ou a prestação de serviços essenciais da cooperativa, em razão da criticidade do serviço prestado, do volume financeiro envolvido, do acesso a dados/informações sensíveis ou da dependência operacional existente.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Incidente de Segurança: um evento que coloca em risco a confidencialidade, integridade, disponibilidade e/ou autenticidade de um sistema de informação ou de

dados que o sistema processa, armazena ou transmite, ou que constitui uma violação ou ameaça iminente de violação das políticas ou procedimentos de segurança. Uma "ameaça iminente de violação" se refere a uma situação em que a organização tem uma base factual para acreditar que um incidente específico está prestes a ocorrer.

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.

Mobile Device Management (MDM): Solução de Gerenciamento de Dispositivos Móveis, utilizada para monitorar, gerenciar e proteger os dispositivos móveis que acessam dados da organização, garantindo a conformidade com as políticas de segurança.

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.

Obsolescência de Ativos de TI: condição na qual um ativo de tecnologia da informação (hardware ou software) não é mais suportado pelo seu fabricante, não recebe atualizações de segurança ou não atende mais aos requisitos de desempenho e conformidade da instituição, representando um risco operacional e de segurança cibernética.

Princípio do Menor Privilégio: conceito que determina que usuários devem ter apenas os acessos estritamente necessários para desempenhar suas funções.

Privacidade: propriedade da informação privada que só pode ser acessada por terceiros com conhecimento e autorização prévios do titular.

Processos Críticos: processo cuja interrupção, falha ou indisponibilidade, após avaliação com base nos critérios de impacto definidos no Plano de Continuidade de Negócios, seja classificada como capaz de gerar impactos relevantes sob a perspectiva financeira, operacional, legal/regulatória e reputacional, devendo, em

razão dessa classificação, ser priorizado nas estratégias de continuidade e recuperação.

Quebra de Segurança: ação ou omissão, intencional ou acidental, que impacta negativamente na segurança da informação e das comunicações.

Rastreabilidade: é a capacidade de traçar o histórico, a aplicação ou a localização de um item por meio de informações previamente registrada.

Segurança da Informação (SI): conjunto de ações que objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Serviços de Computação em Nuvem: abrangem a disponibilidade ao Sistema Uniprime, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços: (i) processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos; (ii) implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; (iii) execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

Serviço Relevante: qualquer serviço cuja interrupção, indisponibilidade, falha ou comprometimento de segurança possa impactar significativamente a continuidade das operações do Sistema, o cumprimento de suas obrigações legais e regulatórias, a proteção de dados e informações, a segurança das transações, a confiança de cooperados, ou que cause prejuízos financeiros e/ou reputacionais.

Singulares: cooperativas filiadas que compõem o Sistema Uniprime.

Sistema Uniprime: conjunto formado pela Uniprime Central Nacional e pelas Cooperativas Filiadas e não filiadas que a integram, atuando de forma coordenada na prestação de serviços financeiros e no atendimento aos cooperados.

Termo de Confidencialidade: compromisso assumido pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

Tratamento da Informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Trilha de Auditoria: registros cronológicos e sequenciais de atividades realizadas em um sistema de informação, que permitem rastrear ações de usuários, acessos a dados e alterações, sendo fundamental para investigações de incidentes e verificação de conformidade.

Uniprime Central Nacional: Cooperativa de crédito de segundo grau, responsável por organizar, coordenar e prover serviços às cooperativas integrantes do Sistema Uniprime.

Usuário: pessoas naturais devidamente autorizadas a acessar ou interagir, incluindo mas não se limitando, aos ativos de informação do Sistema Uniprime, quanto a sua utilização, processamento ou administração.

Vulnerabilidade: uma fraqueza (ou falha) em um sistema, nos procedimentos de segurança do sistema, nos controles internos ou na implementação, pela qual um agente ou evento pode explorar intencionalmente ou acionar acidentalmente a vulnerabilidade para acessar, modificar ou interromper as operações normais de um sistema, resultando em um incidente de segurança ou na violação da política de segurança do sistema.

5 PAPÉIS E RESPONSABILIDADES

Para assegurar a eficácia desta Política e a melhoria contínua da segurança cibernética em todo o Sistema Uniprime, os seguintes papéis e responsabilidades são definidos:

5.1 Conselho de Administração

Compete ao Conselho de Administração:

I. Aprovar esta Política e suas revisões periódicas, garantindo sua atualização no mínimo anualmente;

II. Assegurar a disponibilização dos recursos humanos, tecnológicos e financeiros necessários à sua implementação, manutenção e aprimoramento; e

III. Supervisionar a conformidade regulatória e a efetividade dos controles, tomando ciência dos riscos cibernéticos e dos resultados das auditorias e monitoramentos realizados.

5.2 Diretoria Executiva

Compete à Diretoria Executiva:

I. Assegurar a execução e a eficácia das diretrizes e controles estabelecidos nesta Política em âmbito sistêmico;

II. Supervisionar continuamente as atividades operacionais de segurança cibernética, garantindo o alinhamento com os objetivos da instituição; e

III. Apoiar e viabilizar as ações necessárias ao pleno atendimento dos requisitos regulatórios e estratégicos do Sistema Uniprime.

5.3 Diretor Responsável pela Segurança Cibernética

Compete ao Diretor Responsável pela Segurança Cibernética:

I. Coordenar a implementação e a execução do Plano de Ação e de Resposta a Incidentes, liderando o Grupo de Trabalho em situações de crise;

II. Assegurar a prontidão operacional dos recursos destinados à resposta a incidentes, garantindo o cumprimento das diretrizes estabelecidas; e

III. Zelar pela ausência de conflitos de interesses no desempenho de suas funções de segurança cibernética em relação às demais atribuições na instituição;

IV. Coordenar a prevenção, detecção, resposta e tratamento de incidentes de segurança cibernética no âmbito do Sistema Uniprime;

5.4 Área de Segurança Cibernética da Uniprime Central Nacional

Compete à Área de Segurança Cibernética da Uniprime Central Nacional:

I. Definir diretrizes, padrões técnicos e controles mínimos de segurança cibernética aplicáveis a todo o Sistema Uniprime;

II. Implementar, operar e manter as ferramentas de monitoramento centralizado;

III. Realizar o monitoramento contínuo da conformidade das Cooperativas com esta Política;

IV. Elaborar e disponibilizar relatórios periódicos de segurança e conformidade às áreas de Riscos, Supervisão, Auditoria e à Diretoria; e

V. Promover a melhoria contínua dos controles e processos de segurança cibernética.

5.5 Área de Gerenciamento de Riscos d Conformidade Uniprime Central Nacional

Compete às Áreas de Gerenciamento de Riscos e Conformidade da Uniprime Central Nacional:

I. Apoiar a avaliação dos riscos cibernéticos e realizar o acompanhamento contínuo de indicadores e métricas de segurança;

II. Garantir o contínuo alinhamento regulatório, verificando o estrito cumprimento da legislação e das normas expedidas pelos órgãos reguladores; e

III. Reportar eventuais desvios e fragilidades às instâncias de governança competentes, assegurando a transparência e o suporte às decisões estratégicas.

IV. Validar o cumprimento das diretrizes e controles previstos nesta Política em todas as áreas e Singulares, assegurando o alinhamento com as normas do Banco Central do Brasil;

V. Monitorar indicadores de conformidade e identificar eventuais desvios ou fragilidades nos processos internos que possam comprometer a segurança cibernética e a solidez do Sistema; e

VI. Acompanhar a implementação de planos de ação e de medidas corretivas decorrentes de apontamentos de auditoria, supervisão ou avaliações de riscos.

5.6 Supervisão Auxiliar da Uniprime Central Nacional

Responsável pela supervisão, atuando por meio do acompanhamento de fragilidades ou descumprimento desta Política, com solicitação e monitoramento de planos de adequação, visando sua conformidade e a efetiva implementação de seus processos, controles e estruturas de governança relacionados.

5.7 Singulares

Compete às Singulares:

I. Aprovar esta política, mediante deliberação e aprovação pelo Conselho de Administração, ou na sua ausência, pela Diretoria Executiva;

II. Cumprir integralmente as diretrizes, procedimentos e controles estabelecidos nesta política e em normativos complementares;

III. Implementar, em âmbito local, os controles de segurança cibernética definidos pela Uniprime Central Nacional;

IV. Permitir e viabilizar a instalação, operação e manutenção das ferramentas de monitoramento centralizado;

V. Designar responsáveis locais pela segurança da informação e cibernética;

VI. Reportar imediatamente à área de Segurança Cibernética da Uniprime Central Nacional qualquer incidente, suspeita de violação ou fragilidade de segurança;

VII. Incluir, em adendo a esta Política, os procedimentos aplicáveis ao ambiente local, observando integralmente as diretrizes, princípios e requisitos estabelecidos neste normativo, de forma a assegurar alinhamento, complementaridade e ausência de conflitos com as disposições corporativas.

5.8 Colaboradores e Prestadores de Serviços

Compete aos Colaboradores e Prestadores de Serviços:

I. Cumprir integralmente as diretrizes e orientações de segurança cibernética, observando as regras de comportamento e uso aceitável dos ativos tecnológicos;

II. Zelar pela confidencialidade e proteção das informações a que tiverem acesso em razão de suas atividades profissionais; e

III. Comunicar prontamente qualquer evento, comportamento ou suspeita de violação que possa representar risco à segurança das informações ou à integridade dos sistemas.

5.9 Área ou Responsável Técnico pela Tecnologia da Informação

Compete à Área de Tecnologia da Informação:

I. Implementar os controles de acesso, proteção e classificação das informações em todos os sistemas e ativos de tecnologia da instituição;

II. Operar soluções de rastreamento e monitoramento, viabilizando a geração de evidências e trilhas de auditoria para fins de acompanhamento e conformidade; e

III. Assegurar a disponibilidade e integridade dos ativos, realizando a gestão de vulnerabilidades, atualizações (patch management) e o tratamento técnico de eventos identificados.

6 PRINCÍPIOS

O Sistema Uniprime reconhece os ativos de informação como essenciais à continuidade dos negócios e à confiança de seus cooperados, comprometendo-se a tratá-los com responsabilidade, garantindo a segurança dos dados, bem como a qualidade e a continuidade dos serviços prestados. Suas práticas de segurança da informação fundamentam-se nos seguintes princípios:

I. **Confidencialidade:** proteção dos dados e informações contra acessos não autorizados;
II. **Integridade:** garantia da exatidão e completude dos dados, informações, sistemas e serviços;
III. **Disponibilidade:** garantia de acesso oportuno e contínuo aos dados e sistemas, assegurando a continuidade das atividades e o atendimento aos Cooperados;
IV. **Autenticidade:** garantia de que a informação foi produzida, alterada ou eliminada por pessoas, sistemas ou dispositivos devidamente autorizados;
V. **Conformidade:** aderência às leis, normas e regulamentos internos e externos aplicáveis, promovendo a cultura de integridade e ética;
VI. **Acesso Controlado**: restrição e controle do acesso às informações apenas a colaboradores e prestadores de serviços devidamente autorizados.

7 DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio do Sistema Uniprime, bem como a natureza, a complexidade e criticidade de suas operações, produtos, serviços, e processos, além da sensibilidade dos dados e informações sob sua responsabilidade, devendo ser observadas as seguintes diretrizes gerais de segurança da informação e cibernética:

I. Proteger os dados e informações contra acessos, modificações, destruição ou divulgação não autorizados;

II. Assegurar a disponibilidade e a resiliência dos dados, dos sistemas de informação e dos serviços críticos;

III. Adotar uma gestão de segurança da informação baseada em riscos e alinhada a boas práticas e padrões reconhecidos;

IV. Promover a conscientização e a capacitação em segurança da informação;

V. Assegurar a proteção adequada das informações do Sistema Uniprime e de terceiros;

VI. Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, inclusive no âmbito das diretrizes para a elaboração de cenários de incidentes a serem considerados nos testes de continuidade de negócios;

VII. Responder, gerenciar e aprender com incidentes de segurança;

VIII. Garantir a melhoria contínua da segurança da informação;

IX. Definir procedimentos e controles para a prevenção e o tratamento de incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados sensíveis ou sejam relevantes para as atividades da instituição, em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria Uniprime;

X. Determinar a classificação dos dados e das informações quanto à sua relevância para o Sistema Uniprime;

XI. Fixar os parâmetros a serem utilizados na avaliação da relevância dos incidentes cibernéticos; e

XII. Cumprir integralmente as leis, normas e regulamentos aplicáveis às atividades do Sistema Uniprime.

8 CLASSIFICAÇÃO DE DADOS

Os Dados e Informações objetos da presente Política são classificados de acordo com as categorias abaixo indicadas, considerando a relevância das informações:

I. **Públicos**: informações que não possuem restrições quanto à sua divulgação, podendo ser acessadas por qualquer pessoa sem causar quaisquer consequências danosas aos processos da Uniprime;
II. **Internos**: informação esta que o Sistema Uniprime não possui interesse em divulgar, cujo acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso esta Informação seja disponibilizada, não causa danos sérios à organização;
III. **Confidencial**: informações cuja circulação interna é controlada, por questões estratégicas e de gestão e cuja circulação externa é vedada, pois, se tornadas públicas ou compartilhadas, poderão causar impacto e prejuízos aos negócios ou aos cooperados, bem como gerar vantagens a eventuais concorrentes e perda de Clientes. Este nível envolve todas as Informações e dados referentes aos cooperados do Sistema Uniprime, inclusive dados pessoais;
IV. **Informações Sensíveis**: informações internas e que estão relacionadas às operações ativas, passivas e aos serviços prestados pelo Sistema Uniprime, que: são acobertadas por sigilo bancário, nos termos da legislação aplicável, e/ou cuja perda ou indisponibilidade pode prejudicar ou impedir a adequada prestação de serviços pelo Sistema Uniprime ao cooperado, a realização de operações do Sistema Uniprime e/ou o cumprimento de suas obrigações legais e/ou normativas.

A Uniprime manterá processo contínuo de revisão, avaliação e atualização da classificação das informações, de forma compatível com a evolução dos riscos, dos processos e das exigências legais e regulatórias.

9 INCIDENTES DE SEGURANÇA

O Sistema Uniprime deve estabelecer, manter e testar regularmente uma capacidade contínua, estruturada e abrangente de resposta a incidentes de segurança cibernética e de privacidade de dados. O objetivo estratégico é garantir a rápida preparação, detecção, contenção, erradicação e recuperação de eventos adversos, minimizando os impactos operacionais, financeiros, legais e reputacionais para a cooperativa e seus cooperados, observando as seguintes diretrizes:

9.1 Gestão e Tratamento Contínuo

O Sistema Uniprime deve manter processos formais e centralizados para o registro, classificação, análise e tratamento de incidentes, garantindo que qualquer evento suspeito ou confirmado seja investigado e contido tempestivamente por uma equipe especializada e integrada. Os critérios técnicos de registro, os procedimentos para análise e controle de efeitos, os parâmetros de avaliação de relevância dos incidentes, bem como os critérios e níveis de criticidade utilizados para sua classificação estão definidos e detalhados no Plano de Ação e de Resposta a Incidentes, que integra o arcabouço normativo desta Política.

9.2 Registro e Lições Aprendidas (Melhoria Contínua)

Todos os incidentes relevantes devem ser documentados em um registro central, devendo a organização conduzir análises de causa-raiz (root cause analysis - rca) após a resolução dos eventos críticos. As lições aprendidas devem ser obrigatoriamente incorporadas para a melhoria e adaptação contínua dos controles de defesa e prevenção do Sistema Uniprime.

9.3 Comunicação e Compartilhamento de Ameaças

Devem ser estabelecidos fluxos de comunicação estruturados para garantir a notificação tempestiva a todas as partes interessadas aplicáveis, incluindo a Alta Administração, os titulares de dados e os órgãos reguladores (como Banco Central do

Brasil e ANPD). Adicionalmente, a Uniprime deve manter iniciativas seguras para o compartilhamento de indicadores de ameaças com outras instituições do Sistema Financeiro Nacional, sempre resguardando o sigilo bancário e os segredos de negócio.

9.4 Reporte à Alta Administração

Anualmente, a Uniprime Central Nacional — esta na condição de Sistema — e cada Cooperativa Singular — estas considerando seus ambientes locais —, deverão elaborar relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes, tendo como data-base o dia 31 (trinta e um) de dezembro de cada ano, que deverá ser submetido à aprovação do Conselho de Administração ou, na sua inexistência, à Diretoria Executiva até 31 (trinta e um) de março do ano seguinte ao da data-base, devendo abordar:

I. A efetividade da implementação das ações desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta política;

II. O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes;

III. Os incidentes relevantes relacionados com o ambiente cibernético, ocorridos no período;

IV. Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes de segurança;

V. Os resultados dos testes de intrusão, varreduras e análise periódicas para detecção de vulnerabilidades e os planos estabelecidos para suas correções.

Devido à complexidade e à necessidade de atualização técnica constante, as classificações de impacto operacional — inclusive os critérios para a classificação de incidentes como relevantes —, as métricas de tempo de resposta (SLAs), os fluxos de acionamento do grupo de trabalho, as medidas e procedimentos em casos de incidentes considerados nos testes de continuidade de negócios, os critérios para elaboração relatório anual sobre Plano de Ação e de Resposta a Incidentes e demais

definições operacionais não se exaurem neste documento corporativo e serão regulamentados, detalhados e tratados exclusivamente no Plano de Ação e de Resposta a Incidentes que integra o arcabouço normativo do Sistema Uniprime.

Compete às cooperativas singulares comunicarem a Central sobre qualquer indício, suspeita ou confirmação de incidentes para que as devidas providências sejam tomadas, respeitado o Plano de Ação e de Resposta a Incidentes que contém as diretrizes e orientações necessárias.

10 MEDIDAS DE SEGURANÇA, PROCEDIMENTOS E CONTROLES

Além das diretrizes gerais estabelecidas nesta Política, o Sistema Uniprime deverá adotar medidas de segurança e controles adicionais com o objetivo de reduzir a vulnerabilidade a incidentes de segurança cibernética, proteger os dados e os ambientes tecnológicos e assegurar a continuidade dos negócios e o atendimento aos cooperados, com ênfase na prevenção de incidentes.

10.1 Controle de Acesso e Autenticação

O acesso a dados, sistemas, redes, ambientes tecnológicos e, especialmente, a informações sensíveis, deve observar os seguintes princípios:

I. **Autenticação individual**: o acesso a dados e informações, especialmente aqueles classificados como confidenciais ou sensíveis, deverá ser controlado e limitado ao mínimo necessário, de acordo com o perfil e as atribuições de cada colaborador ou prestador de serviços, por meio de credenciais pessoais, únicas e intransferíveis;
II. **Princípio do menor privilégio**: a concessão de acessos deverá ser baseada no princípio do menor privilégio, garantindo que cada usuário possua apenas as permissões indispensáveis ao desempenho de suas funções, considerando a adequada segregação de funções;
III. **MFA**: autenticação segura através de múltiplo fator de autenticação;

IV. **Autorização prévia**: toda concessão, alteração ou revogação de acessos deverá ser previamente autorizada pela área responsável pelo usuário e formalizada para a área de tecnologia;

V. **Padronização e centralização de acessos**: os acessos deverão ser padronizados e gerenciados de forma centralizada incluindo, obrigatoriamente, autenticação para os seguintes recursos: (i) correio eletrônico corporativo; (ii) acesso às máquinas e aos terminais de trabalho; (iii) sistemas e softwares internos;(iv) e softwares de terceiros;

VI. **Política de senhas**: as senhas deverão possuir complexidade mínima, com composição alfanumérica, além de obedecer a critérios de expiração e renovação periódica;

VII. **Revogação de acessos**: os acessos deverão ser revogados ou bloqueados imediatamente após o término do vínculo trabalhista ou contratual, ou quando não forem mais necessários;

VIII. **Limitação de acessos:** mecanismos para limitar o acesso à rede corporativa a usuários credenciados e a dispositivos autorizados;

IX. **Revisão Periódica:** as permissões de acesso, em especial de colaboradores terceirizados com acesso aos recursos computacionais da instituição, deverão ser revisadas periódica e tempestivamente, no mínimo anualmente.

A gestão de acessos aos softwares e sistemas centralizados é de responsabilidade da Central. Para os softwares e sistemas contratados ou mantidos localmente pelas cooperativas singulares, a gestão de acessos será de responsabilidade da respectiva singular, que deverá implementar e manter controles de autenticação e autorização compatíveis com os requisitos estabelecidos nesta Política. Os procedimentos, critérios e controles adotados no âmbito local deverão ser formalizados em adendo específico a esta Política.

10.2 Criptografia

O Sistema Uniprime deve implementar controles criptográficos robustos e padronizados para proteger a confidencialidade, a integridade e a autenticidade das informações classificadas como Confidenciais e Sensíveis, mitigando riscos de

interceptação, alteração não autorizada ou vazamento de dados. A adoção de tecnologias criptográficas deve observar as seguintes diretrizes:

I. **Criptografia em Trânsito:** toda comunicação, transmissão ou troca de dados sensíveis e confidenciais realizada através de redes públicas, abertas ou não confiáveis (incluindo a Internet) deve ser obrigatoriamente protegida por protocolos criptográficos de rede reconhecidos e atualizados, visando prevenir a interceptação e a leitura de dados em claro;
II. **Criptografia em Repouso:** os dados sensíveis e confidenciais armazenados em ativos de tecnologia – incluindo servidores, bancos de dados, dispositivos móveis e estações de trabalho – devem ser cifrados utilizando algoritmos fortes, de modo a impedir o acesso não autorizado em caso de perda, furto ou comprometimento físico do ativo;
III. **Proteção de Cópias de Segurança (Backups):** o Sistema Uniprime deverá manter cópias de segurança dos dados e informações armazenadas de forma protegida, criptografada e segregada (lógica ou fisicamente), garantindo a irrecuperabilidade dos dados por agentes maliciosos em caso de subtração das mídias ou ambientes de backup;
IV. **Padrões e Algoritmos Reconhecidos:** a organização deve empregar exclusivamente algoritmos, suítes de cifras e comprimentos de chave que sejam validados e recomendados por autoridades e órgãos de padronização internacionais (como o NIST/FIPS), devendo descontinuar e substituir proativamente protocolos obsoletos ou criptograficamente fracos;
V. **Gestão de Chaves Criptográfica:** deve ser estabelecido um processo formal e seguro para o ciclo de vida das chaves criptográficas (simétricas e assimétricas). Isso inclui regras estritas para a geração, distribuição, armazenamento protegido (preferencialmente em cofres digitais ou módulos de segurança de hardware - HSM), rotação periódica, revogação e destruição segura das chaves, assegurando que o comprometimento de uma chave exija resposta imediata a incidentes.

A implementação e a gestão dos controles de criptografia aplicáveis aos softwares, sistemas, ambientes e servidores centralizados são de responsabilidade da Central, observadas as diretrizes e requisitos estabelecidos nesta Política. Para os ambientes,

sistemas e ativos tecnológicos contratados, mantidos ou operados localmente pelas cooperativas singulares, a gestão dos controles de criptografia será de responsabilidade da respectiva singular, que deverá implementar mecanismos compatíveis com os requisitos aqui definidos. Os procedimentos, critérios e controles adotados no âmbito local deverão ser formalizados em adendo específico a esta Política.

10.3 Proteção da Informação

Os mecanismos de monitoramento e controle de segurança da informação devem:

I. Assegurar que os sistemas, dados e informações sejam utilizados exclusivamente para o desempenho das atribuições institucionais e estejam devidamente protegidos;

II. Implementar controles de segurança proporcionais aos riscos, em conformidade com os requisitos mínimos legais, regulatórios e internos, inclusive quando as informações forem acessadas remotamente ou por meio de dispositivos móveis;

III. Adotar técnicas de proteção da informação, como mascaramento de dados ou mecanismos equivalentes, em relatórios, comprovantes e outros documentos compartilhados interna ou externamente, em conformidade com sua classificação;

IV. Estabelecer, manter e evoluir os mecanismos necessários à aplicação dos níveis de classificação e ao tratamento da informação nos sistemas corporativos, documentos, soluções tecnológicas e canais institucionais, podendo, para tanto, adotar ferramentas de apoio e automação, inclusive em comunicações eletrônicas corporativas, observados os critérios definidos nesta Política e nos normativos internos aplicáveis.

A implementação e a gestão dos controles de proteção da informação aplicáveis aos softwares, sistemas, ambientes, servidores e demais ativos centralizados são de responsabilidade da Central, observadas as diretrizes, princípios e requisitos estabelecidos nesta Política.

Para os ambientes, sistemas, ativos e informações contratados, mantidos ou operados localmente pelas cooperativas singulares, a gestão dos controles de proteção da informação será de responsabilidade da respectiva singular, devendo os procedimentos, critérios e controles adotados no âmbito local serem formalizados em adendo específico a esta Política.

10.4 Segurança das informações sensíveis

Os mecanismos de segurança das informações sensíveis devem prever que:

I. O acesso e o compartilhamento de informações sensíveis com prestadores de serviços somente serão permitidos quando estritamente necessários à execução do objeto contratual, devendo ocorrer de forma segura. Tais informações deverão ser armazenadas apenas pelo período necessário ao cumprimento das obrigações contratuais;

II. O compartilhamento e o acesso a informações sensíveis a colaboradores e prestadores de serviços deverão ocorrer de forma segura, previamente autorizada e limitada ao mínimo necessário, mediante contrato ou termo de confidencialidade válido e por meio de conexões privadas e protegidas;

III. O acesso a informações sensíveis deverá ser passível de rastreabilidade, por meio da manutenção de registros e trilhas de auditoria que permitam identificar o responsável, o momento e o recurso acessado. Os registros de acesso deverão conter, no mínimo: (i) identificação do usuário; (ii) data e hora do acesso; (iii) recurso ou informação acessada; e (iv) origem do acesso. Os registros deverão ser mantidos pelo prazo mínimo de 5 (cinco) anos;

IV. Os Prestadores de Serviços que realizarem processamento de Dados Sensíveis deverão observar os mesmos requisitos de rastreabilidade e controle estabelecidos nesta Política;

V. A continuidade do processamento e da disponibilidade das informações sensíveis deve ser mantida, através da adoção medidas preventivas e de contingência compatíveis com os níveis de criticidade.

A implementação e a gestão dos controles segurança das informações sensíveis aplicáveis aos softwares, sistemas, ambientes, servidores e demais ativos

centralizados são de responsabilidade da Central. Para os ambientes, sistemas, ativos e informações contratados, mantidos ou operados localmente pelas cooperativas singulares, a gestão dos controles segurança das informações sensíveis será de responsabilidade da respectiva singular, devendo os procedimentos, critérios e controles adotados no âmbito local serem formalizados em adendo específico a esta Política.

10.5 Prevenção de vazamento de dados e informações

Os bancos de dados são mantidos em rede interna apartado do ambiente dos sistemas operacionais e aplicativos, e mantidos por camadas de segurança. Ao sinal de indício de instabilidade ou tentativa de comprometimento, são gerados alertas para a equipe técnica e contenções através de softwares de segurança.

São implementadas tecnologias para prevenção de perda de dados (Data Loss Prevention - DLP), com o objetivo de monitorar e bloquear a transmissão não autorizada de informações confidenciais e sensíveis para fora do ambiente controlado da cooperativa, minimizando o risco de vazamentos.

A implementação e a gestão para prevenção de vazamento de dados em informações aplicáveis aos softwares, sistemas, ambientes, servidores e demais ativos centralizados são de responsabilidade da Central. Para os ambientes, sistemas, ativos e informações contratados, mantidos ou operados localmente pelas cooperativas singulares, a gestão dos controles segurança será de responsabilidade da respectiva singular, devendo os procedimentos, critérios e controles adotados no âmbito local serem formalizados em adendo específico a esta Política.

10.6 Mecanismos de rastreabilidade

O monitoramento de acessos e das trilhas de auditoria será realizado por meio de soluções tecnológicas específicas, capazes de registrar e acompanhar as sessões dos usuários e o processamento fim a fim dos dados e informações, incluindo acessos

privilegiados e a identificação de falhas de processamento ou comportamentos atípicos, nos ambientes de tecnologia do Sistema Uniprime.

Os registros gerados servirão de base para o monitoramento contínuo pela área de Riscos, bem como para a produção de evidências destinadas à área de Supervisão Auxiliar. Esse processo tem como objetivo prevenir acessos indevidos, detectar eventuais irregularidades e assegurar a integridade, a confidencialidade e a disponibilidade dos dados e sistemas, inclusive por meio da retenção segura das trilhas de auditoria contra modificações não autorizadas.

O período de retenção das informações será definido de acordo com o tipo de processamento realizado, observando-se, sempre que aplicável, os requisitos legais e regulatórios vigentes e as necessidades de rastreabilidade do Sistema Uniprime.

A implementação de mecanismos de rastreabilidade aplicáveis aos softwares, sistemas, ambientes, servidores e demais ativos centralizados são de responsabilidade da Central. Para os ambientes, sistemas, ativos e informações contratados, mantidos ou operados localmente pelas cooperativas singulares, será de responsabilidade da respectiva singular prover tais mecanismos, devendo os procedimentos, critérios e controles adotados no âmbito local deverão serem formalizados em adendo específico a esta Política.

10.7 Prevenção e detecção de intrusão

O Sistema Uniprime deve estabelecer e manter uma capacidade de monitoramento contínuo, estruturado e proativo (Continuous Monitoring) para identificar, analisar e responder tempestivamente a eventos adversos de segurança, garantindo a proteção da infraestrutura, dos endpoints e dos dados organizacionais, em conformidade com as seguintes diretrizes:

I. Manter internamente ou por meio de provedor de serviços de segurança gerenciados (MSSP), um Centro de Operações de Segurança (SOC – Falcon) operando ininterruptamente em regime 24x7. Este centro deverá contar com

equipe capacitada, responsável por monitorar o tráfego de rede, detectar anomalias e conduzir a triagem inicial de alertas e incidentes cibernéticos;

II. A implantação de soluções avançadas para detecção e prevenção de intrusões na rede e plataformas de Detecção e Resposta de *Endpoints* em todos os ativos tecnológicos críticos. Estas soluções, a exemplo dos padrões atuais da instituição, devem ser configuradas para não apenas alertar, mas atuar de forma ativa e autônoma no bloqueio de atividades maliciosas e movimentações laterais;

III. O monitoramento deve ser apoiado por ferramentas automatizadas de correlação de eventos (SIEM), responsáveis por centralizar a coleta de *logs* (registros de auditoria) de múltiplas fontes, aplicando inteligência e orquestração para identificar padrões de ataque complexos em tempo real;

IV. A seleção, configuração e as regras de detecção das ferramentas de monitoramento deverão passar por avaliações e aprimoramentos contínuos, garantindo que o Sistema Uniprime incorpore novos Indicadores de Comprometimento (IoC) e permaneça protegido contra táticas de ameaças emergentes, independentemente do fabricante da tecnologia subjacente adotada.

10.8 Detecção de Vulnerabilidades

Com o objetivo de detectar vulnerabilidades na infraestrutura, sistemas e aplicativos, bem como identificar e corrigir tempestivamente falhas de segurança, serão realizados testes periódicos por empresa especializada, independente, imparcial e contratada para essa finalidade, em conformidade com as melhores práticas de segurança da informação e exigências regulatórias.

Para tanto, serão executados os seguintes testes, no mínimo, duas vezes ao ano:

I. Teste de Intrusão no Ambiente Tecnológico (Pentest BlackBox): destinado à avaliação da segurança do perímetro externo e da infraestrutura exposta, simulando ataques sem conhecimento prévio do ambiente;

II. Teste de Intrusão em Sistemas e Aplicativos (Pentest GrayBox): destinado à avaliação da segurança das aplicações críticas, simulando ataques com conhecimento parcial do ambiente;

III. Prevenção de intrusão através da utilização de ferramenta de proteção contra softwares maliciosos.

As vulnerabilidades identificadas deverão ser tratadas e formalizadas através de plano de ação para correção. Nos casos em que não for possível a eliminação total da vulnerabilidade, deve ser apresentado o documento de avaliação do risco para ciência e decisão de aceitação do risco.

Os testes de intrusão a serem aplicados nos ambientes das cooperativas singulares serão contratados e coordenados pela Central, podendo ser executados de forma centralizada ou direcionada às singulares, conforme planejamento de segurança. As cooperativas singulares deverão apoiar a execução dos testes, assegurando o acesso aos ambientes necessários e a implementação tempestiva dos planos de correção decorrentes dos resultados identificados.

10.9 Gestão de Vulnerabilidades e Atualizações

O Sistema Uniprime deve estabelecer e manter um processo contínuo, estruturado e proativo de gestão de vulnerabilidades e atualizações de segurança aplicável a todos os seus ativos de tecnologia, infraestrutura, sistemas e aplicativos.

Este processo tem como objetivo prevenir a exploração de falhas de segurança conhecidas e assegurar a integridade e a disponibilidade dos serviços, devendo contemplar as seguintes diretrizes:

I. Implementar ferramentas e processos para a execução de varreduras contínuas e automatizadas visando a identificação tempestiva de vulnerabilidades nos ambientes internos e externos, complementando a realização de testes de intrusão (Pentests) periódicos por empresas especializadas;

II. Assegurar que todas as vulnerabilidades identificadas sejam devidamente registradas, avaliadas e classificadas quanto ao seu nível de criticidade e risco para o negócio, utilizando metodologias e padrões reconhecidos de pontuação de risco (ex: CVSS);

III. Estabelecer Acordos de Nível de Serviço (SLAs) rigorosos e formalizados para a aplicação de atualizações (*patches*) de segurança, determinando prazos máximos para a mitigação das falhas com base em sua respectiva classificação de risco (ex: prioridade máxima e prazos exíguos para vulnerabilidades críticas);

IV. Exigir que todas as atualizações de software, firmware e sistemas operacionais sejam, obrigatoriamente, homologadas e validadas em um ambiente de testes (não produtivo) previamente à sua implantação no ambiente de produção, visando garantir a estabilidade das operações e mitigar riscos de indisponibilidade sistêmica;

V. Estabelecer que eventuais exceções à aplicação de correções – motivadas por incompatibilidade técnica, risco severo à operação ou indisponibilidade de atualização pelo fabricante (obsolescência) – deverão ser formalmente documentadas, justificadas tecnicamente e acompanhadas pela imediata implementação de controles compensatórios aprovados pelas áreas de Segurança Cibernética e de Riscos.

As obrigações aqui estabelecidas competem igualmente às cooperativas singulares no que tange à sua infraestrutura local.

10.10 Proteção contra software malicioso

O Sistema Uniprime utiliza ferramenta de proteção contra softwares maliciosos, adotada com o objetivo de prevenir, detectar e responder a ameaças que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações e dos ativos tecnológicos.

A solução implementada contempla, entre outros recursos, a proteção de endpoints, mecanismos de prevenção e mitigação de ransomware, detecção de atividades

maliciosas – incluindo ataques de negação de serviço (DDoS) –, bem como o monitoramento contínuo de eventos de segurança.

Todas as máquinas do Sistema Uniprime, independentemente de conexão à rede, devem possuir a ferramenta padrão de proteção ativa. A gestão e o monitoramento desses controles são de responsabilidade da área de Tecnologia da Informação, que realiza o registro, a análise e o tratamento dos eventos identificados.

10.11 Armazenamento e Backup dos dados e das informações

O processamento e armazenamento de dados ocorrerá apenas em ambientes tecnológicos com rotina de backup, de modo a permitir a restauração adequada de tais dados, garantindo a continuidade do negócio. Esta medida visa prevenir alterações não autorizadas e serve como base para a geração de relatórios de acompanhamento.

O backup das máquinas virtuais é realizado semanalmente, aos sábados, a partir das 4h, com retenção mínima de 15 dias em disco. Os bancos de dados são submetidos a backup diário do tipo full, executado durante a madrugada, além de backups incrementais realizados a cada 30 minutos. A cópia primária desses backups é mantida em disco por até 60 dias. Adicionalmente, é realizada a cópia do backup full em fitas, com retenção por prazo indeterminado.

O Servidor de Arquivos do Data Center está incluído no backup semanal das máquinas virtuais e conta, ainda, com rotinas de backup dedicadas, realizadas duas vezes ao dia, às 7h e às 12h, com retenção aproximada de 45 dias. Esses backups utilizam o recurso de *shadow copies*.

O processo de restauração dos bancos de dados é executado automaticamente em dias úteis pela própria ferramenta de backup. As bases do Sistema Uniprime restauradas são testadas diariamente pelas equipes de Tecnologia da Informação, com o objetivo de validar a integridade e a disponibilidade das informações.

As rotinas de backup são realizadas pela central nos ambientes centralizados, sendo de responsabilidade de cada cooperativa filiada ao sistema prover mecanismos e rotinas de teste e restauração de backup nos sistemas e redes próprios da cooperativa.

As rotinas de backup e os testes de restauração dos sistemas e ambientes locais são de responsabilidade da cooperativa singular, devendo ser implementados, executados e monitorados em conformidade com as diretrizes, princípios e requisitos estabelecidos nesta Política. A singular deverá assegurar a periodicidade adequada, a integridade dos dados e a efetividade dos processos de recuperação, bem como manter registros que comprovem a realização dos testes e a capacidade de restauração dos sistemas sob sua responsabilidade. Os critérios e procedimentos, adotados no âmbito local deverão ser formalizados em adendo específico a esta Política.

10.12 Ativos de Tecnologia

Para preservar a integridade da infraestrutura tecnológica, o Sistema Uniprime estabelece e mantém perfis de configuração segura para todos os seus ativos de tecnologia, garantindo a proteção contra acessos indevidos e a redução da superfície de ataque.

I. **Gestão do Ciclo de Vida e Atualizações:** o gerenciamento dos ativos é realizado por meio de processo formal, contemplando inventário, monitoramento de obsolescência e aplicação regular de correções de segurança (patch management). Esse processo visa mitigar riscos operacionais e assegurar que softwares e firmwares permaneçam em versões suportadas e protegidas.
II. **Configuração e Padrões de Segurança:** a implementação de novos recursos tecnológicos deve assegurar (a) a configuração adequada dos serviços estritamente necessários para o suporte às atividades institucionais e (b) a alteração mandatória de senhas de fábrica e de outros padrões de configuração original do fabricante que possam ser utilizados para acessos indevidos.

Adicionalmente, a Uniprime adotará ferramentas para o registro e controle de ativos não geridos diretamente pela TI, mantendo inventário completo e monitoramento contínuo com vistas à mitigação de riscos.

Os ativos sob gestão direta da cooperativa singular deverão ser formalmente inventariados e documentados, com registro atualizado contendo, no mínimo, suas características, responsável e finalidade de uso.

Essas informações deverão ser encaminhadas à Central e mantidas permanentemente atualizadas, sendo obrigatória a comunicação de alterações, substituições ou novas aquisições, de forma a assegurar a integridade, a rastreabilidade e a atualização contínua do inventário corporativo de ativos.

10.13 Mecanismos de proteção de rede

Os mecanismos de proteção da rede contemplam:

I. a segmentação de rede, resguardando, em especial, o ambiente de produção e os recursos computacionais que suportam processos críticos;

II. regras de *firewall*, assim como o monitoramento de conexões, evitando tentativas de conexão com sistemas de informação provenientes de ativos de tecnologia localizados fora da rede;

III. a definição de critérios para o estabelecimento e o monitoramento de conexões com ambientes externos, em especial em horário noturno e em dias não úteis;

IV. identificação e prevenção de conexões indevidas com ambientes externos à instituição oriundas de recursos tecnológicos da instituição;

V. a implementação e manutenção de processos e ferramentas para identificação, análise, tratamento e controle de eventos atípicos no ambiente de produção, abrangendo, como exemplos, o estabelecimento de VPN e tentativas de acesso privilegiado a recursos computacionais, com monitoramento reforçado em horário noturno e em dias não úteis;

VI. medidas para restringir o acesso a redes corporativas apenas a dispositivos ou ativos de tecnologia devidamente autorizados.

Nos ambientes locais das cooperativas, a implementação e a gestão dos mecanismos de proteção de rede serão de responsabilidade da respectiva singular, que deverá assegurar a adoção de controles compatíveis com os requisitos estabelecidos nesta Política. Os procedimentos, adotados no âmbito local deverão ser formalizados em adendo específico a esta Política.

10.14 Gestão de certificados digitais

O Sistema Uniprime estabelecerá processos e ferramentas para a gestão segura do ciclo de vida dos certificados digitais, contemplando:

I. acompanhamento contínuo do uso de certificados e assinaturas digitais, integrando os mecanismos de rastreabilidade que permitam identificar a origem e o momento das transações realizadas;

II. implementação de procedimentos para a guarda segura e controles de acesso físico e lógico às chaves privadas sob responsabilidade da instituição, utilizando ferramentas que impeçam o seu compartilhamento indevido entre usuários ou prepostos;

III. garantia de validação tempestiva de certificados revogados perante as respectivas autoridades certificadoras, assegurando a integridade das comunicações e assinaturas

Os procedimentos, adotados no âmbito local para a gestão dos certificados digitais, deverão ser formalizados em adendo específico a esta Política.

10.15 Requisitos de segurança para a integração de sistemas de informação por meio de interfaces eletrônicas

Todas as interfaces eletrônicas a serem disponibilizadas à fornecedores, parceiros e associados, devem seguir critérios de segurança que contemplem o estabelecimento de canais seguros de conexão, criptografia de dados em trânsito e rotação de credenciais.

10.16 Inteligência de Ameaças e Monitoramento Contínuo

O Sistema Uniprime deve estabelecer e manter um programa contínuo e proativo de Inteligência de Ameaças para mapear e mitigar riscos externos antes que afetem os sistemas, os cooperados ou a reputação da instituição, observando as seguintes diretrizes:

I. **Monitoramento Contínuo e Proativo:** a área de Segurança Cibernética, apoiada por ferramentas automatizadas ou empresas especializadas, deve realizar o monitoramento contínuo em fontes abertas (OSINT), fóruns ilícitos, Deep Web e Dark Web em busca de indícios de exposição (IoE), tais como: vazamento de credenciais corporativas, bases de dados, dados de cartões, códigos-fonte, ou menções não autorizadas da marca Uniprime;

II. **Integração Defensiva:** as informações e Indicadores de Comprometimento (IoCs) obtidos por meio das ações de inteligência devem ser tempestivamente aplicados e integrados às ferramentas de proteção do Sistema Uniprime, visando o bloqueio preventivo de acessos ou atividades maliciosas;

III. **Gatilho de Resposta a Incidentes:** a confirmação de vazamento de informações sensíveis, dados pessoais ou credenciais da Uniprime na Deep Web ou Dark Web deve ser tratada como um incidente de segurança imediato, acionando o Plano de Ação e de Resposta a Incidentes e desencadeando otificações compulsórias às áreas de Compliance, Jurídico e ao Encarregado pelo Tratamento de Dados Pessoais (DPO);

IV. **Investigações Seguras (Isolamento Lógico):** é estritamente proibido o acesso direto às redes da Deep Web e Dark Web a partir de dispositivos, credenciais ou redes corporativas padrão. Quaisquer análises ou investigações conduzidas internamente por profissionais autorizados devem ocorrer exclusivamente através de máquinas e infraestruturas dedicadas, logicamente e fisicamente isoladas do ambiente produtivo, prevenindo rastreabilidade reversa ou contaminação por artefatos maliciosos.

10.17 Gestão de prestadores de serviço

Os contratos com prestadores de serviço e terceirizados deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, e formalizem termo de ciência quanto às diretrizes desta Política, que garantam que os profissionais:

I. Tenham conhecimento e cumpram esta Política;
II. Zelem e protejam o sigilo das informações;
III. Cumpram as normas legais que regulamentam a propriedade intelectual e a proteção de dados e a normas vigentes relacionadas à segurança cibernética e afins do Banco Central do Brasil;
IV. Utilizem os dados da instituição ou os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da instituição, apenas para as finalidades objeto do contrato de prestação de serviço;
V. Notifiquem imediatamente qualquer violação desta Política ou outras normas.

As contratações realizadas diretamente pelas cooperativas singulares, devem respeitar as mesmas regras contidas nesta Política.

10.18 Gestão de Riscos na Cadeia de Suprimentos

O Sistema Uniprime deve gerenciar ativamente os riscos de segurança cibernética e de privacidade introduzidos por terceiros, fornecedores e parceiros de negócios (Cadeia de Suprimentos), garantindo que os serviços terceirizados operem com níveis de segurança equivalentes aos adotados internamente, em conformidade com as seguintes diretrizes:

I. **Avaliação de Criticidade e Risco:** fornecedores e parceiros devem ser categorizados com base na criticidade dos serviços prestados e no volume/sensibilidade dos dados acessados. Fornecedores críticos devem passar por avaliações rigorosas de segurança previamente à sua homologação, nos termos do Procedimento de Enquadramento de Fornecedores;

II. **Requisitos Contratuais de Segurança:** todo contrato que envolva o processamento, armazenamento ou trânsito de informações do Sistema Uniprime deve conter cláusulas expressas de confidencialidade, privacidade, níveis de serviço (SLAs), notificação tempestiva de incidentes e obrigações de conformidade regulatória;

III. **Requisitos em Cadeia:** deve ser exigido contratualmente que os fornecedores diretos imponham e garantam controles de segurança equivalentes a qualquer de seus subcontratados que venham a processar dados da Uniprime;

IV. **Direito de Auditoria e Validação:** prever contratualmente o direito de auditar (Right to Audit) seus fornecedores relevantes, o que pode ser satisfeito mediante inspeções diretas, avaliações contínuas de postura cibernética ou por meio da exigência de relatórios e certificações independentes de mercado;

V. **Monitoramento e Revisão Contínua:** o desempenho e as práticas de segurança dos fornecedores críticos devem ser monitorados e revisados periodicamente, garantindo a mitigação de eventuais deficiências apontadas e o distrato seguro (com recolhimento e expurgo de dados) em caso de encerramento da prestação do serviço.

As contratações realizadas diretamente pelas cooperativas singulares, devem respeitar as mesmas regras contidas nesta Política.

10.19 Aquisição, Desenvolvimento e Manutenção Segura de Sistemas

As medidas previstas nesta Política, deverão ser observadas na adoção de novas tecnologias, no desenvolvimento de sistemas, na contratação de serviços e no relacionamento com terceiros que tratem dados ou desempenhem atividades relevantes para o Sistema Uniprime.

Para os sistemas desenvolvidos internamente, deve ser assegurada a proteção contra alterações indevidas, com o objetivo de evitar a exposição de dados sensíveis. O acesso ao código-fonte das aplicações deve ser devidamente controlado e protegido, em conformidade com a classificação da informação estabelecida. Apenas colaboradores formalmente autorizados podem acessar o código-fonte, devendo esse

acesso estar sujeito a mecanismos de controle de versão e rastreabilidade, garantindo a integridade, confidencialidade e adequada gestão das modificações realizadas.

O desenvolvimento de sistemas por parte de terceiros, incluindo aqueles contratados pelas cooperativas singulares, deverá ser controlado e auditado por pessoal técnico da Uniprime Central, garantindo a observância das mesmas práticas de desenvolvimento seguro aplicadas internamente, especialmente quando tais sistemas forem executados em recursos computacionais da própria instituição, e assegurados por termo de confidencialidade.

10.20 Segurança Física e Ambiental

O Sistema Uniprime deve estabelecer diretrizes e controles de segurança física e ambiental para proteger as instalações físicas, os ativos tecnológicos e as informações sensíveis e confidenciais contra acessos não autorizados, danos, furtos ou interferências que possam comprometer a continuidade dos negócios. Tais medidas devem contemplar as seguintes diretrizes:

I. **Controle de Acesso Físico:** O acesso às áreas seguras e de processamento de informações críticas deve ser estritamente controlado, restrito a colaboradores formalmente autorizados e protegido por mecanismos de controle de acesso;
II. **Gestão de Visitantes e Terceiros:** em especial às cooperativas singulares, deve ser exigida a identificação formal, e quando aplicável, o acompanhamento (escolta) de visitantes, prestadores de serviços e terceiros durante a permanência nas áreas internas da cooperativa;
III. **Mesa Limpa e Tela Limpa:** os colaboradores e parceiros devem garantir o recolhimento e a guarda segura de documentos físicos confidenciais e mídias removíveis quando as mesas estiverem desocupadas. Os equipamentos e estações de trabalho devem estar configurados com o bloqueio automático de tela após um período definido de inatividade;
IV. **Posicionamento de Equipamentos:** os equipamentos críticos devem ser instalados ou posicionados em áreas fisicamente protegidas, minimizando os

riscos de danos ambientais, interceptação de dados ou acesso visual não autorizado por parte de pessoas não credenciadas;

V. **Termos e Condições de Emprego:** todo indivíduo, antes de receber credenciais de acesso aos sistemas da Uniprime, deverá formalizar o aceite em Termos de Confidencialidade (NDAs) e aderir às regras de comportamento e uso aceitável dos ativos tecnológicos;

VI. **Recolhimento de Ativos:** nos casos de desligamento ou encerramento de contrato, todos os ativos de propriedade da cooperativa devem ser imediatamente recolhidos.

10.21 Diretrizes de Uso de Inteligência Artificial (IA) e GenAI

O Sistema Uniprime deve estabelecer diretrizes, processos e controles para o uso seguro, ético, transparente e confiável de soluções de Inteligência Artificial (IA) e Inteligência Artificial Generativa (GenAI), mitigando riscos cibernéticos, vazamento de dados, vieses discriminatórios e violações de propriedade intelectual, devendo observar as seguintes regras:

I. Uso Aceitável e Proteção de Dados: é expressamente proibida a inserção, submissão ou o processamento de dados pessoais, dados sensíveis, informações financeiras confidenciais ou códigos-fonte de propriedade do Sistema Uniprime em ferramentas, plataformas ou assistentes públicos de Inteligência Artificial Generativa não homologados pela Uniprime Central Nacional;

II. Homologação e Avaliação de Riscos: a aquisição, o desenvolvimento ou a adoção de soluções sistêmicas baseadas em Inteligência Artificial, sejam elas fornecidas por terceiros ou desenvolvidas internamente, devem ser precedidas de rigorosa avaliação pelas áreas de Segurança Cibernética, Riscos e Privacidade, assegurando que o modelo é seguro, resiliente e possui controles contra manipulação de dados e injeção de comandos;

III. Supervisão Humana: decisões críticas de negócios, análises de crédito ou respostas a incidentes geradas ou suportadas por Inteligência Artificial não devem ser executadas de forma inteiramente autônoma. Tais processos devem prever etapas de supervisão, validação e revisão prévia dos resultados por

colaboradores com competência e autoridade necessárias, visando evitar alucinações sistêmicas ou decisões imprecisas;

IV. Transparência e Interação com o Cooperado: o Sistema Uniprime garantirá a transparência na utilização de IA. Quando cooperados ou usuários interagirem diretamente com assistentes virtuais ou quando processos de tomada de decisão forem baseados de forma relevante em sistemas autônomos, as partes afetadas deverão ser comunicadas de maneira clara e acessível;

V. Propriedade Intelectual e Ética: a implementação de IA ou o treinamento de modelos internos deve observar estritamente a legislação de direitos autorais e propriedade intelectual, bem como adotar salvaguardas e testes para impedir que a tecnologia gere conteúdos ofensivos, ilegais ou que promovam tratamentos injustos e discriminatórios.

Devido à abrangência, complexidade e rápida evolução das tecnologias de Inteligência Artificial e GenAI, as regras detalhadas de desenvolvimento, as diretrizes éticas de uso, os métodos de avaliação de risco algorítmico e as obrigações regulatórias não se exaurem neste documento e poderão ser definidas, detalhadas e regidas m documento próprio, a qual complementará a estrutura de governança corporativa do Sistema Uniprime.

10.22 Comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional – RSFN

Para fins desta Política e em conformidade com a regulamentação vigente, o serviço prestado para a comunicação eletrônica de dados na RSFN é considerado serviço relevante para fins da aplicação das regras sobre a contratação de serviços de processamento, armazenamento de dados e computação em nuvem. Esta classificação aplica-se independentemente da forma de conexão utilizada pelo Sistema e abrange os casos em que o prestador forneça serviços de processamento de mensagens no âmbito do SFN e do Sistema de Pagamentos Brasileiro – SPB.

O Sistema Uniprime adota o modelo *on-premises para* Comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional – RSFN e cumpre integralmente todos os requisitos técnicos exigidos, incluindo:

I. Uso de múltiplos fatores de autenticação para o acesso administrativo aos ambientes Pix e Sistema de Transferência de Reservas – STR;

II. Monitoramento do uso de credenciais e certificados digitais, bem como estabelecimento de controles para a guarda dessas informações, especialmente as utilizadas no âmbito do Sistema de Pagamentos Instantâneos – SPI;

III. Mecanismos de validação da integridade fim a fim das transações, assegurando que os dados não tenham sido corrompidos ou manipulados durante o processo de geração dessas mensagens;

IV. Vedação do acesso de empresas prestadoras de serviços a terceiros às chaves privadas associadas a certificados digitais utilizados pela instituição para a assinatura de mensagens;

V. Isolamento físico e lógico do ambiente Pix dos demais sistemas da instituição, garantindo que, em caso de uso de serviços de computação em nuvem, seja mantida instância dedicada e apartada de outros ambientes; e

VI. Isolamento físico e lógico do ambiente STR dos demais sistemas da instituição, mantendo instância dedicada e apartada dos demais ambientes inclusive em cenários de uso de computação em nuvem.

A comunicação é realizada através de duas redes distintas sendo um fornecedor responsável por cada link, seguindo o Catálogo de Serviços, o Manual de Redes e o Manual de Segurança do SFN.

10.23 Conexão a Sistemas do Mercado Financeiro – SMF

No caso de conexão como participante de Sistemas do Mercado Financeiro (SMF) autorizados a operar, o Sistema Uniprime implementará e observará controles de segurança específicos para a prevenção, detecção e resposta a fraudes, garantindo a segurança e a integridade das operações realizadas nesses ambientes.

10.24 Continuidade dos negócios

O processo de gestão de Continuidade de Negócios, está definido no Plano de Continuidade de Negócios, incluindo a realização de testes periódicos de continuidade e recuperação. Esse processo visa minimizar impactos decorrentes de incidentes críticos, assegurar a recuperação de ativos de informação e restabelecer as operações a um nível aceitável, com base na análise de impacto nos negócios, mapeamento de processos críticos, identificação de recursos essenciais e definição de estratégias de recuperação.

As cooperativas singulares devem manter Plano de Continuidade de Negócios próprio considerando o porte, a complexidade e o risco de suas operações, respeitando as diretrizes aqui estabelecidas e evitando conflito ou sobreposição de processos.

11 OBRIGAÇÕES DAS COOPERATIVAS E MONITORAMENTO PELA UNIPRIME CENTRAL NACIONAL

As Cooperativas, filiadas ou não, são corresponsáveis pela segurança cibernética do Sistema Uniprime, devendo observar integralmente as diretrizes, controles e procedimentos estabelecidos nesta Política, bem como nos normativos internos complementares. A Uniprime Central Nacional mantém estrutura e mecanismos destinados à supervisão, ao monitoramento e à avaliação do cumprimento desta Política, com o objetivo de preservar a segurança, a resiliência operacional e a solidez do Sistema Uniprime.

11.1 Obrigações das Cooperativas

As cooperativas devem:

I. Colaborar de forma ativa e contínua para assegurar o pleno funcionamento, a abrangência e a efetividade das ferramentas de monitoramento de segurança cibernética em seus respectivos ambientes tecnológicos;

II. Aderir e cumprir integralmente as diretrizes, controles e procedimentos estabelecidos nesta Política;

III. Elaborar e incluir no adendo a esta Política diretrizes, critérios e procedimentos próprios abrangendo o ambiente e infraestrutura própria e local, considerando sua realidade operacional e tecnológica e respeitando as regras estabelecidas nesta Política;

IV. Elaborar e incluir no adendo ao Plano de Ação e de Resposta a Incidentes, critérios e procedimentos próprios abrangendo o ambiente e infraestrutura própria e local, considerando sua realidade operacional e tecnológica e respeitando as regras estabelecidas nesta Política;

V. Elaborar Plano de Continuidade de Negócios Próprios, respeitando as diretrizes desta Política, contemplando as contingências necessárias para reestabelecimento sistêmico e operacional, considerando o porte, a complexidade e os riscos relacionados à sua infraestrutura local;

VI. Comunicar imediatamente à área de segurança cibernética da Uniprime Central Nacional através do canal de e-mail: infosec@uniprimecentral.com.br; quaisquer descumprimentos desta Política, bem como toda e qualquer suspeita de incidente, vulnerabilidade, intrusão em sistemas, infraestrutura ou acesso indevido a dados, garantindo seu adequado registro, tratamento e resposta de forma centralizada e coordenada;

VII. Adotar medidas tempestivas para mitigação de riscos e tratamento de vulnerabilidades identificadas, conforme orientações da Uniprime Central Nacional;

VIII. Assegurar que contratações de produtos, serviços ou soluções tecnológicas realizadas, estejam em conformidade com as diretrizes desta Política e com os requisitos mínimos de segurança cibernética aplicáveis;

VII. Elaborar relatório anual de resposta a incidentes de acordo com as diretrizes e prazos estabelecidos.

11.2 Monitoramento e Supervisão pela Uniprime Central Nacional

A Uniprime Central Nacional mantém estrutura e mecanismos destinados à supervisão e ao monitoramento contínuo do cumprimento desta Política, por meio de ferramentas

de segurança centralizadas e soluções corporativas aplicáveis a todo o Sistema Uniprime. Tais mecanismos incluem:

I. **Gestão Centralizada de Segurança:** soluções para inventário de ativos, controle de acessos e geração de trilhas de auditoria, abrangendo a Central e as Singulares.
II. **Prevenção de Vazamento (DLP):** ferramentas para apoiar a classificação dos dados e implementar controles que impeçam o vazamento de informações confidenciais e sensíveis.
III. **Rastreabilidade de Acessos:** monitoramento de sessões e de acessos privilegiados no Active Directory (AD) e no Sistema de Tecnologia Uniprime (STU), gerando evidências para a Supervisão e assegurando a integridade e disponibilidade dos sistemas.

O monitoramento aplica-se prioritariamente aos ambientes e serviços tecnológicos centralizados ou compartilhados, incluindo: canais transacionais; o ambiente STU; operações de cartões e meios de pagamento; e-mail e mensageria; sistemas de antivírus; e monitoramento da marca em canais oficiais e não oficiais.

Para fins de mitigação de riscos, toda nova contratação de solução tecnológica local pelas Singulares deve ser submetida à avaliação técnica prévia da Uniprime Central Nacional, que possui a prerrogativa de vetar a contratação caso os requisitos mínimos de segurança não sejam satisfeitos.

12 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem deve ser precedida de avaliação formal da capacidade do prestador em assegurar a confidencialidade, integridade, disponibilidade e recuperação das informações, mediante análise de controles de segurança, continuidade de negócios, níveis de serviço, certificações e requisitos contratuais,

devendo tal avaliação ser devidamente documentada e aprovada pelas áreas competentes.

O estudo formalizado de avaliação de relevância e risco, bem como o parecer técnico da Área de Tecnologia da Informação da Central, constituem pré-requisitos para a deliberação do Conselho de Administração quanto à contratação, assegurando que a decisão seja baseada em análise documentada e compatível com a regulamentação vigente.

A avaliação prévia da relevância do serviço de processamento e armazenamento de dados e de computação em nuvem a ser contratado, deverá ser documentada e levará em consideração (i) a criticidade do serviço; (ii) a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado; e (iii) a classificação dos dados e das informações quanto à relevância.

Devido à complexidade técnica e à necessidade de atualização constante, o detalhamento das cláusulas obrigatórias e os requisitos para contratação, não se exaurem nesta Política e são regulamentados em documento próprio que integra o arcabouço normativo do Sistema Uniprime.

13 CULTURA DE SEGURANÇA CIBERNÉTICA

A Uniprime promoverá, de forma contínua, ações de conscientização, capacitação e treinamento de segurança da informação e segurança cibernética, destinadas a colaboradores e prestadores de serviços, conforme cronograma definido pela área responsável, assegurando o comprometimento da alta administração com a melhoria contínua dos processos e controles relacionados ao tema.

Adicionalmente, os profissionais da área de Tecnologia da Informação e os técnicos responsáveis pela função deverão participar de capacitações técnicas compatíveis com suas funções e responsabilidades, de modo a manter o nível adequado de conhecimento e atualização.

A Uniprime também promoverá, de forma periódica, a divulgação de orientações de segurança digital aos seus cooperados, incluindo boas práticas e medidas essenciais para a utilização segura de produtos e serviços financeiros, com o objetivo de mitigar riscos cibernéticos, assegurando a prestação clara e acessível de informações sobre precauções necessárias no ambiente digital.

As cooperativas singulares deverão incluir no adendo a esta Política, a previsão de treinamentos próprios aos técnicos responsáveis pela função de sua infraestrutura local, assim como as divulgações de orientações próprias aos seus cooperados sobre segurança digital.

14 PENALIDADES E MEDIDAS DISCIPLINARES

O descumprimento das disposições estabelecidas nesta Política, bem como de normas, procedimentos e diretrizes dela decorrentes, sujeitará os responsáveis à aplicação de medidas disciplinares e penalidades cabíveis, sem prejuízo das responsabilidades civis, administrativas e penais previstas na legislação vigente.

No âmbito das Singulares, o descumprimento desta Política poderá ensejar, adicionalmente, a adoção de medidas de supervisão, recomendações formais, planos de ação corretivos, sanções e outras providências definidas pela Uniprime Central Nacional, em conformidade com o modelo de governança e supervisão do Sistema Uniprime.

15 ACOMPANHAMENTO E CONTROLE DA EFETIVIDADE

O Sistema Uniprime institui mecanismos de acompanhamento e de controle destinados a assegurar a implementação e a efetividade desta Política, do Plano de Ação e de Resposta a Incidentes e dos requisitos para contratação de serviços de nuvem, incluindo:

I. Definição de rotinas de revisão, testes de segurança e manutenção de trilhas de auditoria que permitam a rastreabilidade das ações de implementação;

II. Estabelecimento de indicadores de desempenho (KPIs) e de risco (KRIs) adequados para mensurar o nível de conformidade e a eficácia dos controles adotados; e

III. Rito formal para a identificação de lacunas e a correção tempestiva de eventuais deficiências detectadas pelos mecanismos de controle.

16 DISPONIBILIDADE DE DOCUMENTOS AO BANCO CENTRAL DO BRASIL

O Sistema Uniprime deverá manter à disposição do Banco Central do Brasil, pelo prazo mínimo de 5 (cinco) anos, os seguintes documentos e informações:

I. A presente Política de Segurança Cibernética e o Plano de Ação e de Resposta a Incidentes;

II. As atas de reunião do Conselho de Administração ou da Diretoria contendo as aprovações e revisões destes documentos;

III. O Relatório Anual sobre a implementação do Plano de Ação e de Resposta a Incidentes;

IV. A documentação referente à avaliação de relevância e capacidade de prestadores de serviços de nuvem;

V. Os contratos de prestação de serviços relevantes (contados 5 anos após a extinção do contrato);

VI. Dados e registros dos mecanismos de acompanhamento e controle;

VII. Documentação com os critérios que configuram situação de crise; e

VIII. Resultados de testes de intrusão e os respectivos planos de ação para correção de vulnerabilidades (contados a partir da execução do teste).

17 ATUALIZAÇÃO E DIVULGAÇÃO

Esta Política deverá ser revisada no mínimo anualmente, ou sempre que houver alterações na legislação aplicável ou mudanças nas práticas de negócios.

Deve ser aprovada pelo Conselho de Administração ou, na sua ausência, pela Diretoria Executiva, e amplamente divulgada internamente, mediante formalização de termo de ciência por parte dos colaboradores, administradores e membros da Diretoria, bem como publicada no site institucional de todas as cooperativas do Sistema.

Os fornecedores e prestadores de serviços que, em razão de suas atividades, tenham acesso a informações, dados, sistemas ou processos relacionados ao sistema Uniprime deverão formalizar Termo de Confidencialidade e Responsabilidade, comprometendo-se a observar as disposições desta política.

Quadro de Atualizações

Atualização Versão 1.2
Revisão total do conteúdo; atualização normativa e reestruturação.
Aprovada em 29/05/2026

Adendo das Singulares

Nome da Cooperativa: Uniprime Greencred

Este adendo possui caráter complementar à presente Política, devendo ser utilizado para formalização de procedimentos, controles, fluxos, responsáveis e demais informações específicas aplicáveis ao ambiente operacional, tecnológico e organizacional da cooperativa singular, no que se refere:

I. Medidas de Segurança, Procedimentos e Controles

a) Controle de Acesso e Autenticação:
- todos os usuários estão no Active Directory (AD) da Uniprime Central; possuímos controle biométrico facial onde o acesso está limitado, dependendo da função do funcionário a um horário pré-estabelecido;

b) Criptografia:
- utilizamos a ferramenta ESET Full Disk Encryption para criptografar arquivos armazenados; vamos utilizar também a criptografia do Microsoft 365 E5;

c) Proteção da Informação:
- nossas informações são protegidas por antivírus (Eset e CrowdStrike Falcon); nossa rede possui firewall; estamos com equipamentos atualizados com a versão Windows11 PRO; todos os usuários estão no Active Directory (AD) da Uniprime Central; estamos no processo de implantação do **Microsoft 365 E5** onde toda segurança vai ser efetuada pela ferramenta;

d) Segurança das Informações Sensíveis:
- possuímos diferentes níveis de acessos a dados; os acessos aos sistemas são aditáveis; acessos a equipamentos são monitorados; Information Protection & DLP do Microsoft 365 E5;

e) Prevenção de Vazamento de Dados e Informações:

- os dados e sistemas críticos sómente são acessíveis de dentro das nossas instalações onde ocorre o monitoramento por câmeras e biometria; utilização do Insider Risk Management do Microsoft 365 E5;

f) Mecanismos de Rastreabilidade:

- vamos utilizar o Audit do Microsoft 365 E5;

g) Detecção de Vulnerabilidades:

- vamos utilizar o Microsoft Defender XDR do Microsoft 365 E5;

h) Gestão de Vulnerabilidades e Atualizações:

- o sistema antivírus está configurado para diariamente efetuar varreduras; o sistema operacional também está configurado para buscar atualizações; softwares e aplicativos são constantemente atualizados;

i) Armazenamento e Backup dos Dados e das Informações:

- o armazenamento é efetuado e o servidor criptografado e backup em ssd criptografado;

j) Ativos de Tecnologia:

- todos os ativos tem controle interno e quando são descontinuados todas as informações são retiradas; alguns equipamentos (smartphone) possuem sistema de localização e segurança em caso de roubou ou extravio;

k) Mecanismos de Proteção de Rede:

- possuímos firewall onde somente equipamentos cadastrados conseguem entrar na rede; o datacenter é monitorado por câmeras e alarme e acessado por controle biométrico facial;

l) Gestão de Certificados Digitais:

- os certificados são guardados em pastas criptografadas e com senha pin de 6 dígitos;

m) Gestão de Prestadores de Serviço:
- temos mais de 2 prestadores para serviços semelhantes;

n) Gestão de Riscos da Cadeia de Suprimentos:
- possuímos 22 fornecedores para atender a Cooperativa;

o) Aquisição, Desenvolvimento e Manutenção Segura de Sistemas:
- são efetuados pela Uniprime Central.

II. Continuidade dos Negócios:
- possuímos outras unidades que conseguem dar continuidade dos negócios; possuímos backups de todos os equipamentos de infraestrutura; possuímos backups dos links de dados.

III. Cultura de Segurança Cibernética:
- efetuamos periodicamente treinamentos para os colaboradores e também enviamos documentação de boas práticas para os fornecedores.

As disposições aqui estabelecidas deverão observar integralmente as diretrizes, princípios e requisitos definidos na Política de Segurança Cibernética do Sistema Uniprime, não podendo gerar conflito, sobreposição ou descaracterização das responsabilidades e controles institucionais estabelecidos pela Central.

O presente adendo deve ser parte integrante desta Política, aprovado em sua totalidade pelo órgão deliberativo competente e compartilhado com a Uniprime Central Nacional, e pelo Conselho de Administração da Uniprime Greencred, em reunião realizada no dia 17 de agosto de 2026.