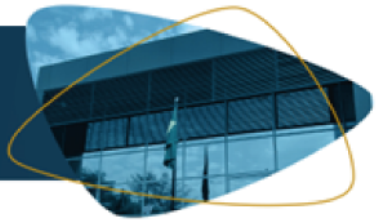
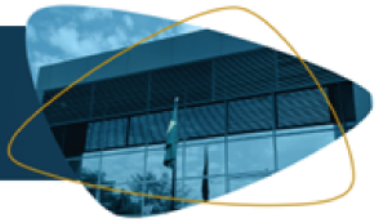


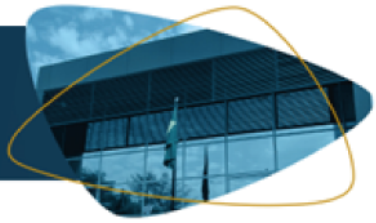
UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

Uniprime cooperativa de crédito	**POLÍTICA DE SEGURANÇA CIBERNÉTICA**	
Elaborado por: Uniprime Central Nacional – Setor de Controles Internos		Data da Criação: 18/04/2016
Aprovador por: Conselho de Administração	Ata n.º **236**	Data Aprovação: 30/01/2024
Início da vigência: 18/04/2016	Revisado em: 30/01/2024	



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

SUMÁRIO



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

1. INTRODUÇÃO

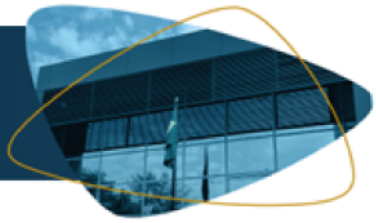
O presente documento estabelece diretrizes gerais e específicas para proteger a confidencialidade, a integridade e a disponibilidade das informações de propriedade do Sistema Uniprime e delineia a estratégia por meio da qual a segurança da informação seja um atributo relevante para a proteção dos ativos, inclusive os ativos Intangíveis, da organização.

~~A~~ direção da Uniprime reconhece a vital importância da definição dos controles de segurança cibernética e da informação e sua procedimentalização em seus processos internos, especialmente naqueles que dizem respeito a clientes, fornecedores e parceiros de negócio.

Esta Política demonstra o compromisso da Uniprime e da sua alta administração em zelar e tratar as informações de seus cooperados quanto à segurança e privacidade de seus dados além de estar em conformidade com as principais regulamentações vigentes.

2. OBJETIVO GERAL

A Política de Segurança Cibernética da Uniprime, visa assegurar a confidencialidade, a integridade e a disponibilidade de dados e sistemas de informações utilizados pela Cooperativa, na prestação de seus serviços e execução de seu objeto social, bem como definir medidas e procedimentos de forma a reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético e garantir a devida proteção dos dados e transações realizadas pelos seus cooperados, bem como zelar pelo dever de sigilo das operações de instituições financeiras conforme Lei complementar nº 105/2001 e a observância à Resolução CMN nº 4.893 de 26/02/2021 de e suas disposições futuras.



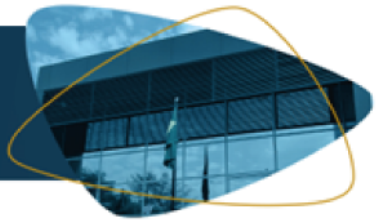
UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

Esta Política visa ainda, identificar possíveis violações de segurança cibernética, por meio da definição de ações sistemáticas de detecção, tratamento e prevenção de Incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, a fim de mitigar, assim, os Riscos Cibernéticos, garantindo, ainda, a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por falhas ou desastres.

3. OBJETIVOS ESPECÍFICOS

A presente Política deverá ser cumprida e respeitada por todos os Colaboradores, e Prestadores de Serviços da Uniprime. Neste sentido, a Política e a governança da informação irão:

I. Proteger a confidencialidade, integridade e disponibilidade das informações e dos dados da Uniprime, contra acessos, modificações, destruições ou divulgações não autorizadas;
II. Adotar uma abordagem considerada e baseada em riscos para o gerenciamento de segurança da informação;
III. Estabelecer uma cultura de consciência de segurança dentro da Uniprime, garantindo que todos os envolvidos tenham as habilidades e a consciência para gerenciar e proteger as informações;
IV. Garantir à Uniprime e a terceiros que as informações estejam devidamente protegidas;
V. Alinhar-se a padrões reconhecidos e boas práticas;
VI. Responder, gerenciar e aprender com os incidentes de segurança da informação para reduzir a probabilidade e o impacto dos incidentes;
VII. Permitir a melhoria contínua na segurança da informação.



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

4. FUNDAMENTAÇÃO LEGAL

Esta Política foi baseada na Resolução CMN nº 4.893 de 26/02/2021, que dispõe sobre a Política de Segurança Cibernética e sobre os requisitospara a contratação de serviços de processamento e armazenamento de dados, computação em nuvem; o Estatuto Social da Uniprime Central Nacional, que define as diretrizes gerais para funcionamento e operações da Uniprime e o Plano de Continuidade de Negócios que define as regras e medidas visando a continuidade dos negócios em situações adversas, a fim de proteger a marca, a reputação, as informações e a conformidade com os requerimentos de órgãos reguladores e legislações.

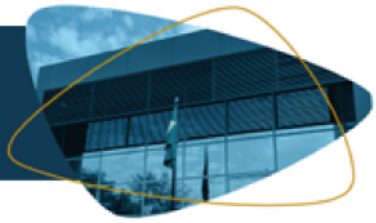
5. DEFINIÇÕES

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

II. **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;

III. **Ativo da Informação**: pessoas, documentos, materiais, equipamentos, meios de armazenamento, transmissão e processamento, ferramentas, sistemas de informação e tudo que manuseie a informação, inclusive ela própria, bem como os locais onde se encontram esses meios;

IV. **Ativos intangíveis:** são as propriedades da instituição que, ao contrário, são difíceis de se ver, de se tocar, mas que se percebe: são suas marcas, a qualidade de sua administração, sua estratégia, sua capacidade de se comunicar com o mercado e com a sociedade, são valores e princípios morais, é a percepção de perenidade que ela transmite, é uma boa governança corporativa, sua capacidade de atrair e reter os melhores talentos, sua capacidade de inovação, seu estoque de conhecimentos;



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

V. **Ativos tangíveis:** são os bens de propriedade da instituição que são concretos, que podem ser tocados. São os imóveis, as máquinas, os estoques etc. (capital físico e financeiro);

VI. **Auditoria:** atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões;

VII. **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;

VIII. **Cliente –** Usuário dos serviços e/ou produtos e empresas contratantes dos serviços fornecidos pelo Sistema Uniprime. Para a Uniprime são considerados clientes: as cooperativas filiadas, as cooperativas conveniadas e os cooperados;

IX. **Colaborador:** é o funcionário, estagiário, voluntário, aprendiz ou parceiro da instituição que está na Uniprime para colaborar, ajudar, contribuir e não necessariamente só cumprir uma jornada de trabalho ou honrar simplesmente um contrato formal;

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

XI. **Conformidade em SI:** cumprimento das legislações, normas e procedimentos relacionados à SI da organização;

XII. **Continuidade de Negócios:** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e a interrupções das atividades operacionais, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

XIII. **Criptografia:** prática de proteger informações por meio do uso de algoritmos codificados, hashes e assinaturas;

XIV. **Custodiante do Ativo de Informação:** aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertençam, mas que estejam sob sua guarda;

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

XVI. **IDS e IPS:** Acrônimos de Instrusion Detection System e Instrusion 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;

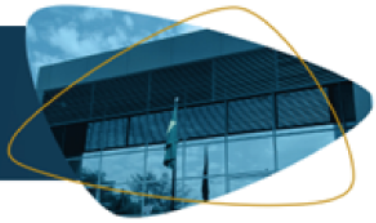
XVII. **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XVIII. ***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;

XIX. **Mecanismos Criptográficos:** são mecanismos que permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utilizam-se, para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração;

XX. **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;

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



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

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

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

XXIV. **Recurso Criptográfico:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXV. **Segurança Empresarial:** é o meio pelo qual se serve a Uniprime para proteger pessoas, bens físicos e instalações, mantendo a continuidade do negócio e impedindo, por meio de ações preventivas e protetivas, riscos que possam ameaçar a organização;

XXVI. **Serviço Relevante:** qualquer serviço que, caso seja interrompido, possa impactar diretamente nas operações perante cooperados, colaboradores, singulares, clientes e central;

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

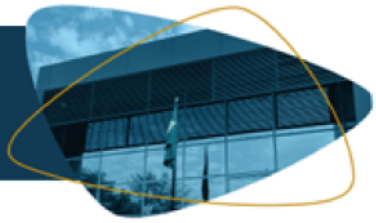
XXVIII. **Singulares Filiadas:** Termo utilizado como referência às Cooperativas Filiadas do Sistema Uniprime;

XXIX. **Sistema Uniprime:** Refere-se ao Sistema Uniprime como um todo, englobando a Uniprime Central Nacional juntamente com suas Cooperativas Filiadas;

XXX. ***Storage:*** é um *hardware* que contém *slots* para vários discos em redundância, capaz de armazenar dados da instituição, ligado aos servidores atravésde ISCSI ou fibra óptica;

XXXI. **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;

XXXII. **Tratamento da Informação:** conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação,



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

destinação ou controle da informação;

XXXIII. **Uniprime Central Nacional:** Cooperativa de crédito de 2º grau, que tem por objetivo organizar e facilitar os serviços de suas cooperativas filiadas e conveniadas;

XXXIV. **Usuário:** qualquer pessoa física que manuseie ativos de informação da Uniprime mediante autorização dos gestores;

XXXV. **Vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente, que pode resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

6. PRINCÍPIOS

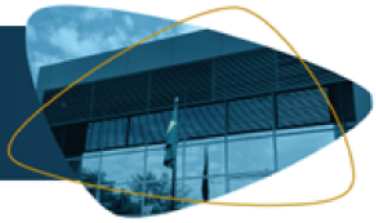
A Uniprime considera que os ativos de informações são os bens mais importantes, portanto, nos comprometemos a tratá-los com responsabilidade, empreender nossos melhores esforços a fim de garantir aos Cooperados a segurança de seus Dados, bem como garantir a qualidade e continuidade dos serviços prestados. Nossas práticas estão fundamentadas de acordo com os princípios indicados a seguir:

I. **Confidencialidade:** é a proteção dos Dados e Informações contra acessos não autorizados;

II. **Integridade:** salvaguarda da exatidão e completeza dos Dados, Informações, sistemas e serviços;

III. **Disponibilidade:** é a garantia de que os Dados e sistemas estarão acessíveis e disponíveis, de modo a garantir a continuidade das atividades da Uniprime e o atendimento ao Cliente e Cooperado;

IV. **Conformidade:** buscar a aderência as leis e normas que regem o sistema Uniprime, sejam elas internas ou externas. Visa, ainda, disseminar a cultura de integridade (Compliance) e estimular comportamentos éticos;

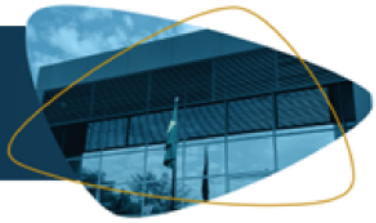


UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

V. **Acesso Controlado**: o acesso aos Dados é restrito e controlado, de modo que somente os Colaboradores, ou Prestadores de Serviços que devem justificadamente ter acesso a uma determinada informação tenham, de fato, referido acesso.

Para isso, os seguintes princípios devem ser respeitados:

I. As informações devem ser identificadas, avaliadas, classificadas e protegidas de acordo com as políticas e padrões acordados;
II. Os controles de segurança devem ser implementados para garantir a confidencialidade, integridade e disponibilidade das informações. Os controles devem ser proporcionais ao risco, mas sempre devem aderir aos padrões mínimos estabelecidos pelas políticas da Uniprime e pelos padrões legais/regulamentares. Os controles de segurança devem ser mantidos quando as informações forem retiradas do local ou acessadas por meio de tecnologias móveis;
III. As transferências de informações para terceiros devem seguir as políticas e serem autorizadas no nível apropriado. Os níveis mínimos acordados de controles de segurança devem ser mantidos. (A transferência para terceiros inclui o uso de serviços em nuvem ou por usuários individuais);
IV. Devem ser implementadas medidas para garantir que os níveis acordados de disponibilidade sejam mantidos no caso de perda acidental deliberada de informações ou sistemas que contenham as informações;
V. Todos os incidentes envolvendo violações reais ou potenciais da Segurança da Informação devem ser relatados e gerenciados de acordo com esta Política e Procedimentos de Incidentes de Segurança da informação. A Uniprime investigará todos os incidentes de segurança e tomará medidas de acordo com aquela política.



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

7. BASES DA POLÍTICA

A presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio da Uniprime, bem como a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição, além da sensibilidade dos dados e das informações sob responsabilidade da Uniprime. Com base na Política de Conduta Ética, no Plano de ação e de Resposta a Incidentes e na Política de Segurança da Informação.

8. ABRANGÊNCIA

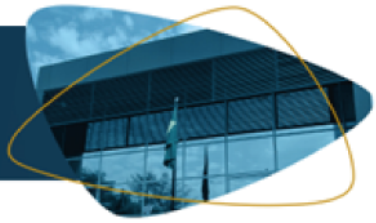
O conteúdo descrito neste documento se aplica aos colaboradores e outros usuários dos recursos de tecnologia da informação, além dos sistemas de informação controlados pela empresa, bem como àqueles controles relacionados à segurança física das instalações contra usuários que não tenham autorização para acessá-los.

Esta Política tem abrangência corporativa na Uniprime Central Nacional e em todas às suas Cooperativas Filiadas, Tomadoras de Serviço, Prestadores de serviço e Colaboradores.

9. 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;



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

II. **Internos** – Informação esta que a 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 Clientes, bem como gerar vantagens a eventuais concorrentes e perda de Clientes. Este nível envolve todas as Informações e Dados referentes aos Clientes da Uniprime, inclusive dados pessoais;

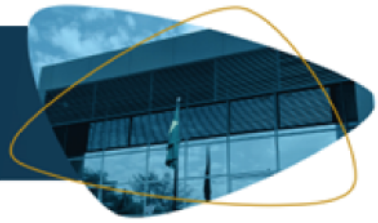
IV. **Informações Sensíveis**: Informações internas e que estão relacionadas às operações ativas, passivas e aos serviços prestados pela Uniprime, que: são acobertadas por sigilo bancário, nos termos da legislação aplicável, a exemplo da Lei Complementar 105/2001; e/ou cuja perda ou indisponibilidade pode prejudicar ou impedir a adequada prestação de serviços pela Uniprime ao Cliente, a realização de operações da Uniprime e/ou o cumprimento de suas obrigações legais e/ou normativas.

A Uniprime manterá um programa de revisão e de classificação contínua das informações.

10. DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA

A presente Política deverá ser cumprida e respeitada por todos os Colaboradores, e Prestadores de Serviços da Uniprime. Neste sentido, deverão ser respeitadas as seguintes diretrizes gerais:

I. Resguardar a proteção dos Dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

II. Realizar a adequada classificação dos Dados, conforme os critérios e princípios indicados no item 9 desta Política;

III. Garantir que os sistemas e Dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;

IV. Garantir a continuidade do processamento das informações Sensíveis;

V. Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os Dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a Dados internos e confidenciais, por meio, dentre outros aspectos:

(i) da manutenção de softwares antivírus e firewall instalados e atualizados;

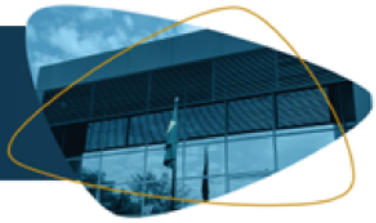
(ii) da manutenção dos programas de computador instalados no ambiente.

VI. Atender às leis e normas que regulamentam as atividades da Uniprime;

VII. Comunicar imediatamente ao Departamento de Controles Internos da Uniprime Central, quaisquer descumprimentos à esta Política, bem como suspeita de intrusão no sistema, infraestrutura ou no acesso aos Dados.

11. MEDIDAS DE SEGURANÇA, PROCEDIMENTOS E CONTROLES

Além das diretrizes gerais supramencionadas, as seguintes medidas de segurança e controles devem ser aplicadas a fim de reduzir a vulnerabilidade a incidentes de segurança e garantir maior segurança aos Dados, aos ambientes lógicos e à continuidade de seus negócios e do atendimento ao Cliente, com foco na prevenção de Incidentes:



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

I. O Colaborador e os Prestadores de Serviços somente deverão possuir acesso aos Dados e Informações internas ou confidenciais após a realização de sua autenticação no sistema da Uniprime, por meio de seu login, com inserção de sua senha pessoal e intransferível, havendo restrição de acesso a informações, em razão do perfil do Colaborador, ou Prestador de Serviço;

II. Os Prestadores de Serviços só poderão ter acesso às informações sensíveis, quando houver expressa autorização do titular dos dados e/ou houver enquadramento em uma das hipóteses previstas na Lei Complementar 105/2001 ou em outra norma que venha a substitui-la, complementá-la ou alterá-la;

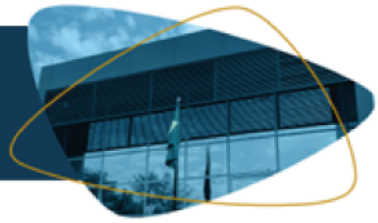
III. Na hipótese de o Prestador de Serviços ou Tomador de Serviço possuírem, em decorrência do Contrato, acesso ao ambiente da Uniprime, quaisquer Informações Públicas, Internas ou Confidenciais, somente poderão ser compartilhadas:

- **a.** na estrita medida necessária para a execução do objeto do contrato;
- **b.** apenas após a assinatura do contrato contendo cláusula de confidencialidade ou após a assinatura de termo de confidencialidade específico; e
- **c.** por meio de conexão privada e segura.

IV. A liberação do acesso aos sistemas da Uniprime deve ter prévia aprovação do Gerente de TI;

V. A liberação do acesso a qualquer endereço de rede deve ter prévia aprovação do Gerente de TI;

VI. Informações Confidenciais e/ou Sensíveis, para esta última, observadas as questões levantadas sobre a necessidade de autorização ou enquadramento nas hipóteses permissivas da Lei Complementar 105/2001, somente deverão ser compartilhadas com o Prestador de serviços, de forma segura;



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

VII. Informações Sensíveis somente devem ser compartilhadas com Prestadores de Serviço, estes últimos na situação em que não atua como intermediário direto, mediante autorização expressa do titular dos dados ou a existência de outra hipótese permissiva na Lei Complementar 105/2001, devendo ser armazenadas apenas durante o período pelo qual estas sejam necessárias à execução dos serviços contratados;

VIII. O acesso a Informações Sensíveis deve poder ser rastreado por meio da manutenção de inventário detalhado dos registros de acesso a referidas informações, contendo o momento, a identidade do responsável e o arquivo acessado;

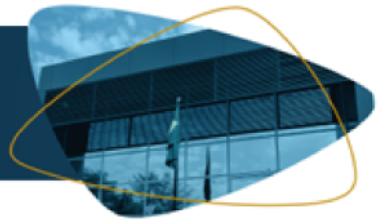
IX. Todos os Colaboradores e Prestadores de Serviço que podem vir a ter acesso aos Dados e Informações Confidenciais devem assinar, obrigatoriamente, termo de confidencialidade ou possuir cláusula de confidencialidade em seus contratos, devidamente validada pelo departamento jurídico;

X. São realizados testes para detecção de vulnerabilidades na infraestrutura da Uniprime, visando a prevenção a intrusões e ao vazamento de informações;

XI. Todos os Dados, incluindo Informações Confidenciais e Sensíveis, devem possuir cópia de segurança, armazenadas de maneira criptografada, segregadas por meio de controles físicos ou lógicos e seguindo os níveis de proteção que razoavelmente se espera do mercado;

XII. Deverão ser realizados treinamentos e avaliações, em periodicidade conforme cronograma de treinamentos emitido pela área de treinamentos a ser definida pelo Diretor Responsável por esta Política, para a devida conscientização, educação e treinamento dos Colaboradores, e Prestadores de Serviços de forma contínua, a fim de que esta Política seja plenamente aplicada, garantindo assim a proteção e confidencialidade dos Dados e Informações e a continuidade do negócio;

XIII. Periodicamente a Uniprime divulgará aos seus Clientes informações acerca das medidas de segurança essenciais à utilização de seus serviços, visando mitigar Riscos Cibernéticos;



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

XIV. Todas as medidas indicadas nesta Política devem ser aplicadas também na adoção de novas tecnologias, na contratação de novos serviços e no desenvolvimento de sistemas de informação pela Uniprime, bem como pelos prestadores de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Uniprime;

XV. A Uniprime realiza o controle de tentativas de acesso e exploração a sistemas por colaboradores, cooperados e clientes.

12. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A contratação, pela Uniprime, de serviços de processamento e armazenamento de dados e de computação em nuvem considerados relevantes nos termos dessa política, se dá de acordo com o disposto na Resolução CMN nº 4.893/2021, conforme cláusulas inseridas em referidos contratos, devendo estes serem devidamente validados.

A decisão de contratação de Serviços Relevantes junto a Prestadores de Serviços externos deverá ser amparada nos seguintes critérios:

I. confirmação da capacidade técnica do Prestador de Serviço de cumprir o quanto disposto nesta Política e na legislação aplicável à segurança cibernética, por meio de auditoria ou da apresentação de declarações e/ou certificações pelo Prestador de Serviço;

II. dificuldade ou impossibilidade técnica ou custo elevado para a execução do Serviço Relevante pela Uniprime em sua própria infraestrutura; e

III. a criticidade e relevância do serviço a ser contratado.

A contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem dispenderá de estudo da área interessada

na contratação quanto ao cumprimento dos requisitos e procedimento previstos no artigo 12 da Resolução CMN nº 4.893 de 26/02/2021, bem como de um parecer técnico da Área de TI da Central, os quais serão apresentados na Reunião do Conselho de Administração.

13. INCIDENTES DE SEGURANÇA

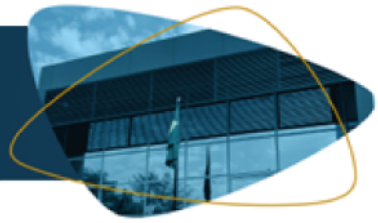
Os Incidentes de segurança serão classificados conforme sua relevância e de acordo com: (i) a classificação dos Dados e Informações envolvidos; e (ii) o impacto na continuidade dos negócios da Uniprime, nas seguintes categorias:

Clas. dos Dados	***Impacto no Negócio**	**Gravidade do Incidente**
Público	Baixo	Simples
Interno	Baixo	Simples
Interno	Médio	Moderado
Confidencial	Médio	Grave
Confidencial	Alto	Gravíssimo
Sensível	Alto	Gravíssimo

São considerados, para a definição do impacto do incidente na continuidade do negócio da Uniprime:

I. **Baixo:** poucas consequências, bem como desdobramentos e reclamações junto às Centrais de Atendimento ao Cliente e a outros canais disponibilizados pela Uniprime, sem, entretanto, afetar o atendimento ao Cliente ou a realização de transações;

II. **Médio:** consequências no atendimento, com desdobramentos relevantes junto às Centrais de Atendimento e potencial de reclamações aos Órgãos Reguladores, especialmente a Autoridade nacional de Proteção de Dados



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

quando o incidente envolver dados pessoais e de Defesa do Consumidor, gerando demanda interna com necessidade de envolvimento das áreas especializadas na adequada resposta ao Cliente lesado/prejudicado, bem com a Órgão Regulador e de Defesa do Consumidor; e

III. **Alto:** consequências relevantes no atendimento, com possibilidade de aplicação de penalidade por parte do Órgão Regulador e de Defesa do Consumidor, bem como de propositura de demandas judiciais, gerando possibilidade de encerramento do vínculo e impedindo o atendimento ao Cliente e/ou a realização de transações.

Os Planos de Resposta, de acordo com a gravidade apurada do Incidente, serão definidos pelo Diretor responsável pela área, com base nas diretrizes constantes do Plano de Ação e de Resposta a Incidentes, as quais serão implementadas por meio do serviço de gerenciamento de tecnologia da informação.

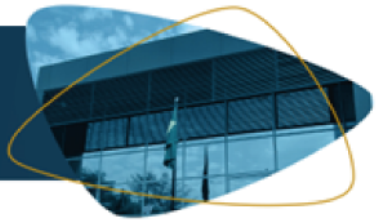
Incidentes deverão ser imediatamente comunicados ao Diretor responsável pela área, para adoção das medidas descritas no Plano de Ação e de Resposta a Incidentes. Em caso de Prestadores de Serviços, a ocorrência do Incidente deve ser imediatamente comunicada ao gestor do contrato na Uniprime.

Quando da ocorrência de Incidente, o Diretor responsável pela área coordenará a adoção das medidas visando a contenção e solução do Incidente, atribuindo responsabilidades às demais áreas envolvidas, englobando, entre outros aspectos, conforme delimitado no Plano de Ação e de Resposta a Incidentes:

I. a análise das causas do Incidente e de seus impactos;

II. as medidas necessárias para estancar o Incidente e controlar seus efeitos;

III. o plano de comunicação do Incidente aos Clientes e às autoridades, sem prejudicar as investigações do ocorrido e a identificação da causa raiz.



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

14. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE OS INCIDENTES RELEVANTES

A Uniprime disponibilizará as informações sobre os seus incidentes relevantes, em especial, seus registros, análises da causa e do impacto e os controles dos efeitos dos incidentes com as demais instituições financeiras e autorizadas a funcionar pelo Banco Central por meio das iniciativas ajustadas entre as instituições, resguardando o sigilo bancário das informações, seus segredos de negócios e privilegiando a livre concorrência entre os participantes do mercado.

15. CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, retornando a operação a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

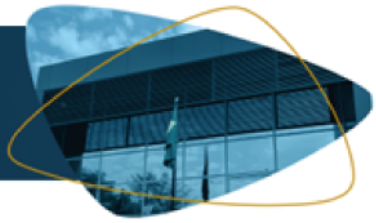
Referido processo deverá considerar, ao menos, os seguintes cenários para a realização de testes de continuidade de negócios:

I. Exploração de possíveis vulnerabilidades que permitam o acesso, a cópia e/ou a extração de Informações e Dados internos e/ou confidenciais do ambiente lógico da Uniprime;

II. Realização de testes de intrusão à base de dados contendo Informações Sensíveis da Uniprime;

III. Tempo de recuperação de acesso a informações de backup em caso de perda de Informações Sensíveis;

IV. Estratégias para a recuperação de Informações Sensíveis e Serviços Relevantes.



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

16. MONITORAMENTO DAS SINGULARES

O monitoramento perante às singulares é realizado pela Uniprime Central apenas nos ambientes, produtos e serviços centralizados – ou seja, nos canais IB, MB e ATM, Sistema de Tecnologia STU, operações com cartões, entre outros. Todos os demais produtos e serviços contratados diretamente pelas singulares, exceto os que envolvam acesso a informações centralizadas, não são de responsabilidade da Central.

Adicionalmente, as contratações de produtos e serviços, devem atender aos requisitos do Formulário de Contratação de Serviços e levados ao conhecimento da Central, a fim de garantir o monitoramento da Política de Segurança Cibernética.

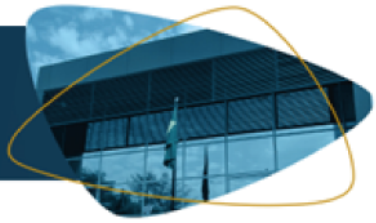
17. CONFORMIDADE

A Uniprime está empenhada em garantir que as estruturas de governança estejam em vigor e comprometida com a melhoria contínua da segurança Cibernética.

Todos os funcionários devem ler, compreender e concordar em cumprir esta política e quaisquer outras políticas e/ou processos relevantes. Qualquer violação desta política, ou de outras que compõem indissociavelmente esta, resultará em procedimento administrativo e em ação disciplinar.

18. PAPÉIS E RESPONSABILIDADES

As diretorias da Uniprime se comprometem com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objeto de pautas recorrentes junto ao Conselho de Administração.



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

19. VIGÊNCIA

Este documento deve ser revisado, no mínimo, anualmente com base em:

I. Resultados de auditorias internas e/ou externas periódicas, avaliações e análises;

II. Revisões de Incidentes de segurança, incluindo ações corretivas e preventivas;

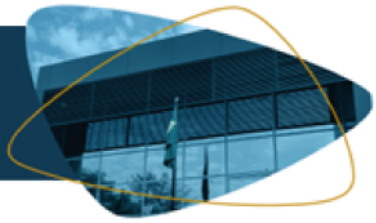
III. Relatórios de não conformidade;

IV. Atualizações dos registros de risco da Uniprime;

Alterações de Legislação e/ou regulamentos.

20. COMUNICAÇÃO

Em caso de dúvidas acerca desta Política, por favor entre em contato com a Uniprime por meio do e-mail politicas@uniprimecentral.com.br.



UNIPRIME CENTRAL NACIONAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Lonrina/PR
www.uniprime.com.br

21. QUADRO DE ATUALIZAÇÕES

Data	Versão	Item Atualizado	Observações
26/09/2019	1.0	Política aprovada.	- Resolução CMN n° 4.658, 26/4/2018. - Ata n.º 184 do C.A.
03/03/2021	1.0	Revisão anual. Não houve alteração de conteúdo.	- Resolução CMN nº 4.658. 26/04/2018, art. 10. - Ata n.º 199 do C.A.
03/08/2022	1.1	Revisão anual. Atualização de acordo com a Resolução CMN nº 4.893/2021.	- Resolução CMN nº 4.893/2021. - Ata nº 216 do C.A.
15/01/2024	1.2	Revisão anual. Atualização completa da política.	- Resolução CMN nº 4.893/2021. - Ata nº 236 do C.A.