



## **1. INTRODUÇÃO**

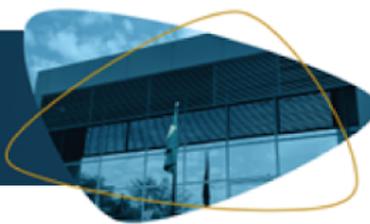
O presente documento estabelece diretrizes gerais e específicas para proteger a confidencialidade, a integridade e a disponibilidade das informações de propriedade do Sistema Uniprime e delinea a estratégia por meio da qual a segurança da informação seja um atributo relevante para a proteção dos ativos,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



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.



## 4. 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;
- 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.

## **5. 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.



## **6. DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA**

A presente Política deverá ser cumprida e respeitada por todos os Colaboradores, e Prestadores de Serviços da Uniprime.

## **7. 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.