

**POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO**  
**UNIODONTO AMAPÁ**

---



**SUMÁRIO**

1. INTRODUÇÃO .....	3
2. OBJETIVO .....	3
3. ABRANGÊNCIA .....	3
4. DIRETRIZES.....	4
5. NORMAS DE SEGURANÇA DA INFORMAÇÃO.....	4
5.1. CLASSIFICAÇÃO DA INFORMAÇÃO.....	4
5.2. CONFIDENCIALIDADE.....	4
5.3. DESCARTE SEGURO .....	4
5.4. ACESSO e SENHAS.....	4
5.5. USO DE EQUIPAMENTOS.....	4
5.6. E-MAIL CORPORATIVO .....	5
5.7. MONITORAMENTO. ....	5
5.8. AVISO LEGAL.....	5
5.9. PROTEÇÃO CONTRA AMEAÇAS.....	5
5.10. TRATAMENTO DE INCIDENTES.....	5
6.CARGOS, FUNÇÕES E RESPONSABILIDADES.....	5
7.SANÇÕES E PUNIÇÕES .....	6
8.CASOS OMISSOS .....	6
9.REVISÕES .....	7
10.GESTÃO DA POLÍTICA.....	7



## 1. INTRODUÇÃO

1.1. A UNIODONTO AMAPÁ reconhece que os dados corporativos, pessoais e sensíveis sob sua guarda constituem ativos estratégicos fundamentais à qualidade e segurança dos serviços prestados.

1.2. A organização está ciente de que o tratamento dessas informações envolve etapas críticas de coleta, armazenamento, processamento e comunicação, passíveis de riscos internos e externos que podem comprometer sua integridade, confidencialidade e disponibilidade.

1.3. Com base nesse entendimento, a UNIODONTO AMAPÁ estabelece a presente Política Geral de Segurança da Informação, em consonância com seu sistema de gestão corporativa, alinhada às melhores práticas do mercado, normas ISO/IEC 27001/27701 e em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

## 2. OBJETIVO

2.1. Estabelecer diretrizes para proteger a informação contra acesso não autorizado, vazamento, alteração, perda ou destruição.

2.2. Promover a **Confidencialidade, Integridade e Disponibilidade** das informações tratadas pela UNIODONTO AMAPÁ.

2.3. Orientar os colaboradores quanto à adoção de comportamentos e controles que assegurem a segurança das informações corporativas e de dados pessoais.

2.4. Prevenir incidentes de segurança, perdas financeiras, danos à reputação e responsabilidades legais.

2.5. Reforçar a cultura organizacional de segurança da informação e conformidade com a LGPD.

## 3. ABRANGÊNCIA

3.1. Esta política aplica-se a todos os usuários de informação da UNIODONTO AMAPÁ, incluindo:

- Prestadores e ex-prestadores de serviços;
- Beneficiários e ex-beneficiários;
- Funcionários e ex-funcionários;
- Credenciados e ex-credenciados;
- Sócios e ex-sócios;



- Qualquer indivíduo que acesse, utilize ou tenha acesso a informações físicas ou digitais da cooperativa.

#### 4. DIRETRIZES GERAIS

4.1. A gestão da segurança da informação deve atuar de forma proativa, antecipando riscos e adotando medidas de proteção compatíveis com o nível de criticidade das informações.

4.2. Todos os dados devem ser tratados com zelo, ética e responsabilidade, conforme suas classificações e finalidades de uso.

#### 5. NORMAS DE SEGURANÇA DA INFORMAÇÃO

##### 5.1. Classificação da Informação

- **Interna:** Informação que, se divulgada, pode prejudicar a cooperativa ou seus clientes.
- **Confidencial:** Informação sigilosa cuja divulgação ou uso indevido pode gerar prejuízos. Deve ser protegida com mecanismos de acesso controlado.

##### 5.2. Confidencialidade

5.2.1 É vedado o compartilhamento de dados corporativos, pessoais ou sensíveis com terceiros fora dos limites contratuais e funcionais estabelecidos.

5.2.2 O descumprimento desta diretriz poderá gerar sanções e punições disciplinares, incluindo demissão por justa causa.

##### 5.3. Descarte Seguro

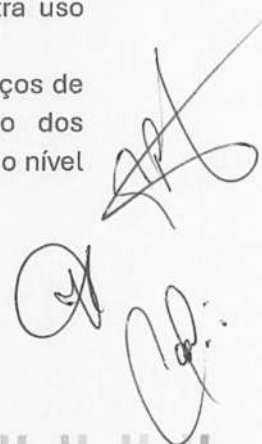
O descarte de informações deve impedir sua recuperação, independentemente do meio (físico ou digital).

##### 5.4. Acesso e Senhas

Os acessos são fornecidos exclusivamente para que os usuários/funcionários possam executar suas atividades laborais.

- 5.4.1 O acesso é pessoal, intransferível e restrito à necessidade funcional.
- 5.4.2 Senhas devem ser sigilosas, trocadas periodicamente e protegidas contra uso indevido.
- 5.4.3 Haverá diferenciação entre os níveis de autorização de acesso ativos/serviços de informação com base em perfis que definem o nível de privilégio dos usuários/funcionários, não podendo por exemplo o empregado ter o mesmo nível de senha do que um gestor.
- 5.4.4 A equipe de TI é responsável pela emissão inicial e suporte aos acessos.

##### 5.5. Uso de Equipamentos



Os equipamentos eletrônicos (computador, e-mail, pendrive, nuvem, token, etc) têm o objetivo específico de permitir aos usuários/funcionários desenvolverem suas atividades profissionais.

- 5.5.1 É proibido o uso pessoal, armazenamento de arquivos particulares e instalação de softwares não autorizados.
- 5.5.2 Equipamentos devem ser bloqueados quando não estiverem em uso.
- 5.5.3 Em caso de qualquer necessidade de manutenção a equipe de T.I deverá ser acionada, especialmente em caso de suspeita de malwares, e outros vírus.

#### 5.6. E-mail Corporativo

- 5.6.1 O e-mail institucional é de uso profissional e monitorado.
- 5.6.2 É vedado o envio de mensagens pessoais ou compartilhamento de informações com domínios externos sem autorização.

#### 5.7. Monitoramento

A cooperativa se reserva o direito de monitorar o uso de seus ativos tecnológicos para garantir a segurança da informação, sem violar direitos fundamentais dos usuários.

#### 5.8. Aviso Legal

O acesso aos sistemas e dados da organização implica ciência e concordância com os termos desta política e suas atualizações.

#### 5.9. Proteção contra Ameaças

- A cooperativa mantém soluções atualizadas contra malwares e outras ameaças.
- Suspeitas devem ser imediatamente reportadas ao setor de TI para contenção.

#### 5.10. Tratamento de Incidentes

- Incidentes devem ser reportados imediatamente ao CGSI e ao setor de TI.
- Devem ser isolados, analisados, documentados e solucionados com base em planos de resposta previamente definidos.

## 6. CARGOS, FUNÇÕES E RESPONSABILIDADES

### 6.1. Comitê Gestor de Segurança da Informação (CGSI)

Composição mínima:

- Representante da Diretoria: Dr. Claudio Calandrini
- Encarregada de Dados (DPO): Tatiara Galvão
- Tecnologia da Informação: André
- Segurança da Informação: Heldecir
- Jurídico: Artur Azevedo



### Responsabilidades:

- Deliberar políticas e ações estratégicas;
- Assegurar recursos e conformidade com a política;
- Promover cultura interna de segurança da informação.

### 6.2. Setor de Segurança da Informação

- Gerir a segurança da informação;
- Propor melhorias e medidas corretivas;
- Tratar incidentes e apoiar o CGSI.

### 6.3. Gestores da Informação

- Gerenciar o ciclo de vida das informações de sua área;
- Controlar acessos e autorizações;
- Formalizar termos de ciência e uso.

### 6.4. Usuários

- Conhecer e cumprir esta política;
- Reportar violações e dúvidas;
- Assinar termo de responsabilidade e uso dos sistemas.

## 7. SANÇÕES E PENALIDADES

7.1. As infrações às diretrizes de segurança serão punidas com base na gravidade e reincidência, podendo incluir:

- Advertência verbal ou escrita;
- Suspensão;
- Demissão por justa causa;
- Responsabilização civil e criminal, conforme previsto no art. 482 da CLT.

7.2. Terceiros e prestadores de serviços estarão sujeitos às penalidades previstas contratualmente.

## 8. CASOS OMISSOS

8.1. Serão analisados e deliberados pelo CGSI.

8.2. A política será constantemente revista e adaptada a novas tecnologias, ameaças e exigências legais.



## 9. REVISÃO

9.1. Esta política será revista anualmente ou sempre que houver mudanças significativas no ambiente regulatório, organizacional ou tecnológico.

9.2. Revisões extraordinárias poderão ser realizadas conforme necessidade identificada pela Diretoria ou CGSI.

9.3 A presente política foi aprovada, no dia 24/10/2022.

9.4 As revisões são observadas no quadro abaixo.

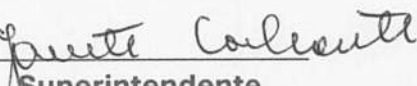
### REVISÕES

<u>DATA DA REVISÃO</u>	<u>ITEM REVISADO</u>	<u>RESPONSÁVEL</u>
07/07/2022	Todos os itens	HUGO FERREIRA
07/07/2025	Todos os itens	TATIARA GALVÃO

## 10. GESTÃO DA POLÍTICA

10.1. Esta política é aprovada pela Diretoria Executiva da UNIODONTO AMAPÁ, com o apoio técnico do Comitê Gestor de Segurança da Informação.

**Presidente**  
  
**Vice-presidente**

  
**Superintendente**



## 9. REVISÃO

9.1. Esta política será revista anualmente ou sempre que houver mudanças significativas no ambiente regulatório, organizacional ou tecnológico.

9.2. Revisões extraordinárias poderão ser realizadas conforme necessidade identificada pela Diretoria ou CGSI.

9.3 A presente política foi aprovada, no dia 24/10/2022.


9.4 Revisada em 07/07/2025 e aprovada pela Diretoria, no dia 07/07/2025.

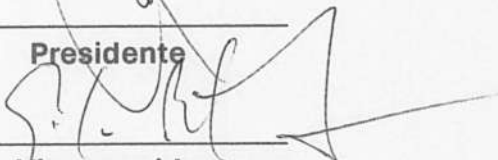
### REVISÕES

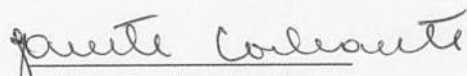
DATA DA REVISÃO	ITEM REVISADO	RESPONSÁVEL
07/07/2022	Todos os itens	HUGO FERREIRA
07/07/2025	Todos os itens	Tatiara Galvão

## 10. GESTÃO DA POLÍTICA

10.1. Esta política é aprovada pela Diretoria Executiva da UNIODONTO AMAPÁ, com o apoio técnico do Comitê Gestor de Segurança da Informação.

  
\_\_\_\_\_  
**Presidente**

  
\_\_\_\_\_  
**Vice-presidente**

  
\_\_\_\_\_  
**Superintendente**

