---

title: “Política de Segurança do Usuário” document_type: “Documentação Legal” system: “Gorgen - Aplicativo de Gestão em Saúde” version: “1.0” status: “Aprovado” last_updated: “26/01/2026”

updated_by: “Manus AI”

> ***Controle de Versão***
>
> | ***Campo*** | ***Valor*** |
> | --- | --- |
> | ***Versão*** | *1.0* |
> | ***Status*** | *Aprovado* |
> | ***Última Atualização*** | *26/01/2026* |
> | ***Atualizado por*** | *Manus AI* |

Política de Segurança do Usuário – Sistema Gorgen

Versão 1.0 | Janeiro 2026

1. Introdução: A Segurança é uma Responsabilidade Compartilhada

No Sistema Gorgen, a segurança dos seus dados é nossa prioridade máxima. Implementamos as mais robustas medidas técnicas para proteger suas informações. No entanto, a segurança é uma parceria. A sua colaboração, adotando práticas seguras no dia a dia, é fundamental para manter a integridade e a confidencialidade da sua conta e dos seus dados de saúde.

Esta política descreve as suas responsabilidades e as melhores práticas que você, como usuário, deve seguir para garantir um ambiente seguro para todos.

2. Gerenciamento de Credenciais: A Chave da Sua Conta

Suas credenciais (CPF e senha) são a porta de entrada para suas informações mais sensíveis. Trate-as com o máximo cuidado.

2.1. Criação de Senhas Fortes

- **Complexidade:** Sua senha deve ter no mínimo 12 caracteres, combinando letras maiúsculas, letras minúsculas, números e símbolos (ex: `!@#$%^&*`).
- **Não use informações pessoais:** Evite usar datas de aniversário, nomes de familiares, seu CPF ou sequências óbvias (ex: `123456` ou `senha123`).
- **Seja único:** Não reutilize senhas de outros sites ou serviços. Se uma senha sua vazar em outro lugar, sua conta Gorgen permanecerá segura.

2.2. Confidencialidade da Senha

- **Nunca compartilhe sua senha:** Nenhum funcionário do Gorgen ou do consultório jamais solicitará sua senha. Se alguém o fizer, recuse e reporte imediatamente.
- **Cuidado onde digita:** Evite fazer login em computadores públicos ou em redes Wi-Fi não seguras.

2.3. Autenticação de Múltiplos Fatores (MFA)

O uso de um segundo fator de autenticação (via aplicativo autenticador ou SMS) é **obrigatório** para perfis com acesso a dados clínicos (Médico) e recomendado para todos os usuários. Ative essa camada extra de segurança nas configurações do seu perfil.

3. Proteção Contra Ameaças Externas

Criminosos digitais utilizam técnicas de engenharia social para enganar usuários e roubar informações. Esteja atento.

3.1. Phishing

Phishing é a tentativa de obter suas informações confidenciais se passando por uma comunicação legítima. Fique alerta a:

- **E-mails ou mensagens inesperadas:** Desconfie de mensagens que pedem para você clicar em um link para "verificar sua conta", "atualizar seus dados" ou que criem um senso de urgência.
- **Remetentes suspeitos:** Verifique o endereço de e-mail do remetente. Comunicações oficiais do Gorgen sempre virão de domínios conhecidos (ex: `@gorgen.com.br`).
- **Links falsos:** Antes de clicar, passe o mouse sobre o link para ver o endereço real. Se parecer suspeito, não clique.

3.2. Segurança do Dispositivo

- **Mantenha seu sistema atualizado:** Instale as atualizações de segurança do seu sistema operacional (Windows, macOS, Android, iOS) e do seu navegador.
- **Use um antivírus:** Mantenha um software antivírus de boa reputação ativo e atualizado em seu computador.
- **Bloqueie sua tela:** Sempre bloqueie seu computador ou celular (`Windows + L` ou `Ctrl + Command + Q`) ao se afastar dele.

4. Uso Responsável da Plataforma

- **Acesso autorizado:** Utilize o sistema apenas para as finalidades para as quais seu perfil foi autorizado. Tentar acessar dados ou funcionalidades fora do seu escopo é uma violação grave.
- **Encerramento de sessão (Logout):** Ao terminar de usar o Gorgen, especialmente em um computador compartilhado, sempre clique em **"Sair"** ou

“Logout” para encerrar sua sessão de forma segura.

5. Reportando um Incidente de Segurança

Se você suspeitar que sua conta foi comprometida, que recebeu uma comunicação falsa ou observou qualquer atividade estranha, aja rapidamente:

1. **Troque sua senha imediatamente** através da função “Esqueci minha senha” na tela de login.
2. **Reporte o incidente** imediatamente ao nosso canal de suporte, fornecendo o máximo de detalhes possível.
    - **Canal de Suporte:** [Definir e-mail ou portal de suporte, ex: segurança@gorgen.com.br]

Sua vigilância e comunicação rápida são essenciais para contermos qualquer ameaça e protegermos toda a comunidade de usuários do Gorgen.

Ao utilizar o Sistema Gorgen, você reconhece ter lido, compreendido e concordado em seguir esta Política de Segurança do Usuário. O descumprimento destas diretrizes pode resultar nas sanções previstas nos Termos de Uso.