



SEGURANÇA E PROTEÇÃO DE DADOS

Aplicativos e Sistemas Glória Virtual

Documento institucional para clientes e parceiros

Versão 1.3 | Julho de 2026

Segurança não é apenas tecnologia. É um processo contínuo de prevenção, controle, monitoramento e responsabilidade.

Compromisso da Glória Virtual

Desenvolver aplicativos e sistemas confiáveis, com proteção de dados desde a concepção, controles proporcionais ao risco e rotinas de continuidade adequadas a cada operação.

01 Nosso compromisso com segurança e privacidade

A Glória Virtual adota segurança por design: a proteção de dados é considerada desde o planejamento do aplicativo ou sistema, e não apenas depois de sua publicação. Cada projeto é analisado conforme os tipos de informação tratados, o perfil dos usuários, as integrações e o impacto potencial de um acesso indevido.

Nossos controles seguem os princípios de finalidade, necessidade, prevenção, transparência, segurança e responsabilização previstos na Lei Geral de Proteção de Dados Pessoais - LGPD.

Importante

Nenhuma tecnologia oferece risco zero. A segurança resulta da combinação entre arquitetura adequada, configuração correta, uso responsável, treinamento das equipes e melhoria contínua.

02 Controles aplicados aos aplicativos e sistemas

CONTROLE	COMO PROTEGE
Criptografia	Proteção das informações durante a transmissão e no armazenamento, reduzindo o risco de leitura indevida.
Conexões seguras	Uso de HTTPS/TLS para proteger a comunicação entre usuários, aplicativos, APIs e serviços autorizados.
Autenticação e perfis	Acesso mediante identificação do usuário e permissões definidas por função, unidade, equipe ou tipo de operação.
Menor privilégio	Cada usuário recebe somente os acessos necessários para executar suas atividades.
Segregação lógica	Regras de acesso ajudam a impedir que usuários visualizem registros de outras empresas, unidades ou pacientes sem autorização.
Gestão de segredos	Chaves de API, tokens e credenciais são mantidos em ambiente protegido e não devem ser expostos no navegador, em repositórios públicos ou em arquivos de backup.

03 Proteção de dados sensíveis

Dados referentes à saúde e dados biométricos vinculados a uma pessoa são considerados dados pessoais sensíveis. Por isso, projetos que tratam esse tipo de informação recebem cuidados adicionais de acesso, retenção, transparência e rastreabilidade.

- Coleta apenas dos dados necessários para a finalidade informada.
- Definição de base legal e responsabilidades junto ao cliente controlador dos dados.
- Acesso restrito a profissionais e perfis previamente autorizados.
- Separação entre dados cadastrais, clínicos, documentos, imagens e registros técnicos quando adequado.
- Prazos de retenção e procedimentos de exclusão definidos conforme a finalidade e as obrigações legais.
- Proteção reforçada para documentos, áudios, transcrições, imagens faciais e registros de atendimento.

Dados de saúde e biometria

O uso desses dados deve ser aprovado no escopo do projeto, documentado nos avisos de privacidade e limitado ao que for realmente necessário.

04 Inteligência artificial com supervisão

A inteligência artificial pode auxiliar no atendimento, classificação de solicitações, agendamentos, transcrição e automação de processos. Em situações críticas, a decisão final deve permanecer sob responsabilidade humana.

- A IA não deve substituir diagnóstico, prescrição ou decisão clínica de profissional habilitado.
- Respostas e automações de maior impacto devem possuir regras, limites e caminhos de atendimento humano.
- Prompts, integrações e registros devem evitar o envio desnecessário de dados identificáveis.
- O cliente deve definir quais colaboradores podem acessar conversas, transcrições e históricos.
- Integrações externas são avaliadas conforme finalidade, segurança e necessidade do projeto.

05 Testes antes da publicação

Antes da entrada em produção, a Glória Virtual recomenda e executa, conforme o escopo contratado, uma revisão de segurança que inclui:

- teste de login, perfis e recuperação de acesso;
- verificação de permissões por registro e por função;
- revisão de páginas, endpoints e arquivos que não podem ser públicos;
- checagem de chaves, tokens e credenciais;
- validação de integrações e fluxos automatizados;
- revisão de mensagens de privacidade, consentimento e atendimento aos titulares.

06 Responsabilidade compartilhada

A proteção das informações depende da atuação conjunta da Glória Virtual, do cliente, dos usuários autorizados e dos provedores de infraestrutura. Cada parte possui responsabilidades específicas.

GLÓRIA VIRTUAL

- Projetar a arquitetura e os controles previstos no escopo.
- Configurar perfis, permissões e integrações com segurança.
- Proteger credenciais técnicas e orientar o cliente.
- Corrigir vulnerabilidades identificadas nos componentes sob sua gestão.

CLIENTE CONTROLADOR

- Definir finalidade, base legal e prazos de retenção.
- Autorizar usuários e revisar acessos periodicamente.
- Treinar colaboradores e proteger senhas e dispositivos.
- Manter avisos de privacidade e canais para os titulares.

USUÁRIOS AUTORIZADOS

- Não compartilhar credenciais ou dados fora dos canais aprovados.
- Utilizar o sistema apenas para finalidades profissionais autorizadas.
- Comunicar acessos suspeitos, erros ou possíveis incidentes.
- Respeitar sigilo profissional e regras internas do cliente.

PROVEDORES DE INFRAESTRUTURA

- Manter controles de segurança compatíveis com os serviços contratados.
- Disponibilizar recursos de continuidade, registro e proteção conforme o plano.
- Comunicar incidentes nos termos contratuais aplicáveis.
- Permitir configurações seguras de identidade, acesso e armazenamento.

07 Monitoramento, continuidade e incidentes

- Monitoramento de falhas, acessos e comportamentos anormais, conforme os recursos do projeto.
- Rotinas de backup e exportação compatíveis com a criticidade das informações.
- Procedimentos para contenção, investigação, correção e prevenção de recorrência.
- Comunicação ao cliente e apoio na avaliação de notificações legalmente aplicáveis.
- Preservação de evidências técnicas e registro das medidas adotadas.

Continuidade do atendimento com inteligência artificial

Em caso de indisponibilidade da LLM principal utilizada no atendimento ao cliente, a Glória Virtual acionará o plano de contingência, configurando uma chave de API de outra LLM compatível e previamente homologada para restabelecer o atendimento no menor prazo possível. A substituição preservará, quando tecnicamente possível, as principais regras e funções do fluxo.

08 Estratégia de backup e continuidade

A Glória Virtual utiliza camadas distintas de backup para proteger o código dos sistemas e os dados operacionais dos clientes. A separação reduz a dependência de um único ambiente e facilita a recuperação em caso de falha, exclusão indevida ou necessidade de migração.

DESTINO	TIPO DE CONTEÚDO	FINALIDADE
GitHub privado	Código-fonte; funções de backend; arquivos de configuração sem senhas; documentação técnica; histórico de alterações e versões.	Versionamento do código, rastreabilidade das mudanças e recuperação de versões anteriores do sistema.
Google Cloud Storage	Exportações do banco de dados; cadastros; agendamentos; registros clínicos quando contratados; documentos; imagens; áudios; transcrições; anexos; relatórios e logs de operação.	Cópia externa dos dados e arquivos, com acesso privado, segregação por cliente, retenção e possibilidade de restauração.
Ambiente de segredos	Senhas, tokens, chaves de API, certificados e credenciais de conexão.	Manter credenciais fora do código e dos arquivos comuns de backup, com acesso restrito e rotação quando necessário.

Separação entre clientes

Os backups são organizados de forma segregada por cliente, projeto ou ambiente. O acesso deve ser concedido somente às identidades técnicas e profissionais autorizados, evitando compartilhamento amplo de pastas, buckets ou repositórios.

Rotina recomendada

CÓPIA	FREQUÊNCIA DE REFERÊNCIA	OBSERVAÇÃO
Código no GitHub	Sincronização contínua ou a cada alteração relevante.	Repositórios privados e separados por projeto ou cliente.
Dados críticos	Conforme a criticidade, preferencialmente em intervalos curtos.	Pacientes, agendamentos, financeiro e registros essenciais exigem menor tolerância à perda.
Backup completo	Duas vezes ao dia: às 12h e às 22h.	Exportação integral com data, horário e validação da quantidade de registros.
Cópia de longo prazo	Mensal, conforme a política de retenção.	Armazenamento protegido e revisão periódica dos prazos legais e contratuais.
Teste de restauração	Periódico.	Um backup só é confiável quando o procedimento de recuperação é testado e documentado.

09 Checklist de segurança para entrada em produção

01	Acessos	Usuários, perfis e unidades revisados; princípio do menor privilégio aplicado.
02	Permissões	Testes confirmam que cada usuário acessa somente os registros autorizados.
03	Dados públicos	Páginas, arquivos e endpoints públicos foram revisados.
04	Credenciais	Chaves e tokens estão protegidos e separados entre teste e produção.
05	Privacidade	Aviso de privacidade, finalidades e canal do titular estão definidos.
06	Dados sensíveis	Saúde, biometria e documentos possuem controles reforçados.
07	Retenção	Prazos de armazenamento, exclusão e anonimização foram definidos.
08	Backups	Código versionado em GitHub privado; dados e arquivos copiados para Google Cloud Storage; restauração testada.
09	Auditoria	Eventos relevantes são registrados conforme a necessidade do projeto.
10	Equipe	Colaboradores receberam orientação de segurança e confidencialidade.

10 Declaração institucional

Compromisso contínuo

A Glória Virtual busca manter seus aplicativos e sistemas protegidos por meio de boas práticas de engenharia, controle de acesso, proteção de credenciais, revisão de configurações, monitoramento, backups externos e atualização contínua.

Este documento apresenta diretrizes e controles de segurança adotados nos projetos da Glória Virtual. Ele não representa garantia absoluta contra incidentes, nem substitui auditoria técnica ou jurídica específica. Os recursos efetivamente aplicados dependem do escopo contratado, da configuração de cada sistema, dos serviços integrados e das práticas operacionais do cliente.

Para projetos que envolvam dados de saúde, biometria, grande volume de dados ou operações críticas, recomendamos uma avaliação específica de impacto, privacidade e continuidade antes da publicação.

GLÓRIA VIRTUALgloriavirtual.com

Inteligência artificial e sistemas personalizados para empresas.

@thiagopetrolina