Política de Segurança da Informação

Última atualização: 8 de julho de 2026 · Versão 1.0

Aviso. Este é um documento operacional da Guvik. Não constitui aconselhamento jurídico e não substitui a análise de um advogado nem os instrumentos contratuais formais aplicáveis a cada cliente ou parceiro. Condições específicas prevalecem quando previstas em contrato assinado.

1. Governança e escopo

Esta Política de Segurança da Informação descreve os controles técnicos e organizacionais adotados pela **GUVIK TECNOLOGIA E INTELIGENCIA ARTIFICIAL LTDA**, inscrita no CNPJ **67.712.906/0001-00**, com sede em **AV BRIG FARIA LIMA, 1811 - Conj 1119 - CEP 01452-001 - JARDIM PAULISTANO - São Paulo-SP** ("Guvik"), para proteger os dados, sistemas e ambientes de seus clientes na plataforma de orquestração de agentes de inteligência artificial ("IA") para SAP (ECC e S/4HANA), acessível pelos domínios dashboard.guvik.ai/app.guvik.ai (aplicação), agent.guvik.ai (API do agente) e parceiros.guvik.ai (Portal de Parceiros).

Esta política se aplica a todos os colaboradores, prestadores de serviço e sistemas envolvidos na operação da plataforma Guvik, e complementa a Política de Privacidade, os Termos e Condições de Inteligência Artificial e o Acordo de Tratamento de Dados (DPA) firmado com cada cliente.

2. Classificação de dados

A Guvik classifica os dados tratados na plataforma nas seguintes categorias, com controles proporcionais à sensibilidade de cada uma:

Categoria	Exemplos	Nível de proteção
Credenciais de conexão SAP	Usuário/senha ou token de conexão ao ambiente SAP do cliente	Máximo — apenas em memória, nunca persistidas em disco (Seção 4)
Conteúdo de conversas e artefatos	Prompts, respostas da IA, código ABAP, documentos gerados	Alto — criptografado em trânsito e em repouso
Metadados de objetos SAP	Nomes, tipos e estrutura de objetos consultados	Alto
Dados de conta e contato	Nome, e-mail, empresa, papel do usuário	Alto
Telemetria de uso	Tokens consumidos, custo, latência, erros	Médio
Dados de parceiros e oportunidades	Cadastro e pipeline no Portal de Parceiros	Alto

3. Controle de acesso

O acesso à plataforma e aos dados nela contidos é controlado por múltiplas camadas:

1. **Autenticação**: realizada via **Firebase** com tokens **JWT**, exigida para acesso à aplicação, à API do agente e ao Portal de Parceiros;
1. **Autorização hierárquica**: perfis definem conjuntos de capacidades; grupos adicionam restrições de conexão SAP e de ferramentas (MCP); usuários recebem um perfil e um grupo, com eventuais exceções específicas; tenants (clientes) podem impor restrições adicionais no nível da organização;
1. **Princípio do menor privilégio**: cada agente, usuário ou integração recebe apenas as permissões estritamente necessárias para executar sua função;
1. **Isolamento por tenant**: conexões SAP, conversas, artefatos e credenciais de um cliente são isolados dos de outros clientes por meio de um componente interno dedicado ("gestor de tenants");

1. **Revisão periódica de acessos**: privilégios concedidos a usuários e integrações são revisados periodicamente para identificar e remover acessos desnecessários.

4. Tratamento especial de credenciais SAP

Em razão de sua sensibilidade, as **credenciais de conexão SAP** informadas pelo usuário recebem tratamento diferenciado:

1. São mantidas **exclusivamente em cache, em memória** do processo do agente, nunca em disco;
1. Possuem **tempo de vida limitado (TTL) de aproximadamente 12 horas**, após o qual expiram automaticamente e exigem nova autenticação;
1. São descartadas em reinícios, atualizações ou reimplantações ("deploys") da plataforma, exigindo que o usuário autentique novamente;
1. Não são compartilhadas com provedores de LLM nem incluídas em prompts enviados a esses provedores;
1. Não são acessíveis por outros tenants, em razão do isolamento descrito na Seção 3.

5. Criptografia em trânsito e em repouso

1. **Em trânsito**: toda comunicação entre o navegador do usuário, a aplicação, a API do agente e os provedores de LLM integrados é protegida por **TLS** (HTTPS);
1. **Em repouso**: dados persistidos (conversas, artefatos, metadados, dados de conta) são armazenados de forma protegida na infraestrutura de hospedagem da Guvik, com controles de acesso restritos à camada de aplicação; credenciais SAP, conforme a Seção 4, não são persistidas em disco e, portanto, não se aplicam a este item;
1. A Guvik avalia periodicamente a adequação dos algoritmos e protocolos criptográficos utilizados frente ao estado da arte.

6. Segurança de aplicação e ciclo de desenvolvimento (SDLC)

1. O desenvolvimento da plataforma segue práticas de revisão de código antes da integração de alterações;
1. Alterações passam por processos de teste automatizado e, quando aplicável, validação manual antes de chegarem a ambientes de produção;
1. Segredos e chaves de API são geridos por meio de variáveis de ambiente e cofres de segredos, nunca versionados em código-fonte;
1. A Guvik busca acompanhar boas práticas reconhecidas de desenvolvimento seguro de software (incluindo referências como o OWASP Top 10) na construção e manutenção de sua plataforma.

7. Gestão de subprocessadores

A Guvik utiliza subprocessadores (fornecedores terceiros) para operar sua infraestrutura e suas funcionalidades de IA, incluindo provedores de nuvem, provedores de LLM e serviços de comunicação. A relação completa, com categoria, finalidade, sede e local de tratamento de cada subprocessador, consta da **Lista de Subprocessadores**, publicada separadamente e atualizada sempre que houver alteração relevante. A contratação de subprocessadores observa exigências mínimas de segurança e proteção de dados compatíveis com esta política.

8. Registro de eventos (logging), auditoria e telemetria

1. A plataforma mantém registros técnicos ("logs") de eventos relevantes para operação, segurança e suporte, incluindo autenticações, chamadas de API e execução de ferramentas pelos agentes;
1. É mantida telemetria de uso de IA (tokens consumidos, custo estimado, erros, status de execução), utilizada para faturamento, suporte e melhoria da plataforma;

1. Casos de suporte podem ser correlacionados a eventos técnicos por meio de um identificador de correlação por requisição, permitindo investigação pontual de incidentes reportados por um cliente;
1. O acesso a logs e registros de auditoria é restrito a pessoal autorizado, observado o princípio do menor privilégio.

9. Resposta a incidentes e notificação

A Guvik mantém um processo de resposta a incidentes de segurança que inclui, conforme aplicável:

1. Identificação e contenção do incidente;
2. Avaliação de impacto, incluindo eventual exposição de dados pessoais;
3. Correção da causa raiz;
4. Comunicação aos clientes afetados e, quando exigido por lei (LGPD, GDPR ou outra legislação aplicável), às autoridades competentes, dentro dos prazos legais cabíveis;
5. Registro e revisão pós-incidente para prevenção de recorrência.

Incidentes de segurança que envolvam dados pessoais de clientes são tratados também em conformidade com o Acordo de Tratamento de Dados (DPA) e a Política de Privacidade.

10. Continuidade de negócio e backup

A Guvik adota rotinas de backup dos dados persistidos na plataforma (excluídas as credenciais SAP, que, por definição, não são persistidas) e mantém procedimentos voltados à continuidade da operação em caso de falhas de infraestrutura, hospedada em **infraestrutura de nuvem contratada pela Guvik**, região **região operacional definida conforme arquitetura vigente**. Testes de recuperação e metas formais de tempo de recuperação (RTO) e ponto de recuperação (RPO) encontram-se em processo de formalização e serão detalhados em versão futura desta política ou em anexo contratual específico.

11. Segurança de pessoas

1. Colaboradores e prestadores com acesso a dados de clientes estão sujeitos a obrigações de confidencialidade;
1. O acesso de colaboradores a ambientes de produção e a dados de clientes segue o princípio do menor privilégio e é revogado imediatamente ao término do vínculo;
1. A Guvik promove conscientização periódica sobre boas práticas de segurança da informação junto à sua equipe.

12. Alinhamento a frameworks de referência

A Guvik toma como referência frameworks reconhecidos de segurança da informação, como a **ISO/IEC 27001** e o **SOC 2**, para orientar a evolução de seus controles internos. **A Guvik ainda não possui certificação formal ISO/IEC 27001 nem relatório SOC 2 vigente. A adoção desses frameworks como certificações formais é um objetivo em avaliação, sem prazo definido.** Esta seção será atualizada assim que houver certificações ou relatórios de auditoria formais disponíveis para compartilhamento com clientes, sob acordo de confidencialidade quando aplicável.

13. Reporte de vulnerabilidades

Pesquisadores de segurança, clientes e parceiros que identifiquem uma potencial vulnerabilidade na plataforma Guvik são incentivados a reportá-la de forma responsável, antes de qualquer divulgação pública, pelo canal:

1. Segurança da informação: **seguranca@guvik.com.br**

A Guvik se compromete a confirmar o recebimento do reporte, investigar a questão com prioridade proporcional ao seu risco e manter o reportante informado sobre o andamento da correção, dentro do possível.

14. Contato

1. Segurança da informação: **seguranca@guvik.com.br**
1. Privacidade e proteção de dados: **privacidade@guvik.com.br**
1. Encarregado/DPO: **dpo@guvik.com.br**
1. Jurídico/comercial: **contato@guvik.com.br**
1. Suporte técnico: **suporte@guvik.com.br**

A versão vigente deste documento é sempre a publicada em **guvik.ai**. Em caso de conflito entre esta versão e uma versão impressa ou anteriormente salva, prevalece a versão publicada no site.