VISÃO GERAL DE SEGURANÇA

Versão 1.0 · publicada em setembro de 2026 · vigente a partir de [dd/mm/2026] · [https://www.ergondata.ai/legal]/seguranca

Esta página descreve, na camada pública, como a plataforma Ergondata é hospedada e protegida. Ela resume os controles adotados e declara com clareza o que ainda está em andamento. A ficha técnica completa de infraestrutura, segurança e conformidade, com diagramas de arquitetura, fluxo de dados e rede, é disponibilizada a clientes e a candidatos a cliente sob acordo de confidencialidade, para avaliação de risco de fornecedor e questionários de segurança. Divergência entre um questionário preenchido e a ficha técnica resolve-se pela correção do questionário.

1. PRINCÍPIOS

1.1 A plataforma foi desenhada para operar processos críticos com agentes de IA governados. Quatro princípios orientam a segurança: isolamento por organização em toda decisão de acesso; negação por padrão, com permissões declaradas para pessoas e para agentes; trilha de auditoria por ação, para humanos e agentes sob a mesma identidade; e custódia de credenciais fora do alcance de agentes, automações e registros.

2. HOSPEDAGEM E INFRAESTRUTURA

2.1 A plataforma é um serviço em nuvem, multi-tenant, hospedado integralmente na Amazon Web Services, na região us-east-1 (Estados Unidos), em conta dedicada da Ergondata. Não há componente instalado no ambiente do cliente, não há implantação por região do cliente e nenhum código é executado no perímetro do cliente: as integrações abrem conexão a partir da plataforma para os sistemas do cliente, com credencial resolvida no momento da chamada.

2.2 A aplicação roda em contêineres gerenciados, sem servidores administrados manualmente, com imagens imutáveis e versionadas, escala automática e rede segmentada: apenas o balanceador de carga é exposto à internet; aplicação e dados ficam em sub-redes privadas, sem endereço público.

2.3 Os bancos de dados são gerenciados, com criptografia em repouso, cópias de segurança automáticas diárias com retenção de 7 dias, recuperação a ponto no tempo e proteção contra exclusão. O armazenamento de objetos tem criptografia padrão e bloqueio total de acesso público; o acesso a arquivos ocorre exclusivamente por URLs pré-assinadas de curta duração.

3. IDENTIDADE E CONTROLE DE ACESSO

3.1 Autenticação com senha protegida por hash moderno, segundo fator (TOTP) configurável como obrigatório por organização e autenticação única corporativa por OIDC (Google e Microsoft). Sessões de curta duração com renovação rotacionada. Chaves de API com permissões granulares para integrações.

3.2 Autorização por papéis com granularidade por recurso, isolamento por organização em toda decisão e negação por padrão: nenhuma leitura ou escrita contorna o motor de políticas. A organização pode restringir o acesso por lista de endereços IP e por janelas de horário.

3.3 Os acessos administrativos da Ergondata são nominais, exigem segundo fator e são integralmente registrados na trilha de auditoria. Não existe conta administrativa compartilhada.

4. CRIPTOGRAFIA E CREDENCIAIS

4.1 Em trânsito: TLS 1.3 na borda; toda integração com terceiros trafega exclusivamente por HTTPS/TLS. Em repouso: bancos de dados e armazenamento de objetos com chaves gerenciadas em serviço de gerenciamento de chaves; objetos com AES-256.

4.2 As credenciais de integração dos clientes ficam em cofre próprio, com criptografia de envelope (AES-256-GCM e chaves gerenciadas), e são resolvidas apenas no momento da chamada: nunca são expostas ao agente, ao fluxo da automação ou aos registros.

5. AGENTES GOVERNADOS

5.1 Cada agente atua na plataforma como identidade própria, com permissões declaradas pelo cliente, dentro de limites que o cliente define, e cada ação é registrada na trilha de auditoria da organização. O cliente decide quais ações um agente executa de forma autônoma e quais exigem aprovação humana; a ampliação do que o agente executa é decisão de governança registrada e reversível. Os dados dos clientes não são utilizados para treinar modelos, próprios ou de terceiros.

6. TRILHA DE AUDITORIA E OBSERVABILIDADE

6.1 Toda ação relevante, de pessoas e de agentes, gera evento imutável na trilha de auditoria da organização, retida por, no mínimo, 12 meses, consultável e exportável pelo cliente. A disponibilidade da plataforma é monitorada continuamente, com relatório por organização no Console.

7. SUBPROCESSADORES E RESIDÊNCIA DE DADOS

7.1 Os terceiros que tratam dados em nome dos clientes constam da Lista de subprocessadores, com função e localização. Os dados da plataforma residem nos Estados Unidos (AWS us-east-1); a transferência internacional é regida pelo Anexo C dos Termos de Licença e pela Política de Privacidade.

8. CONTINUIDADE E RECUPERAÇÃO

8.1 Cópias de segurança automáticas diárias, com retenção de 7 dias e recuperação a ponto no tempo. Objetivos de tempo e de ponto de recuperação (RTO e RPO) não são declarados como compromisso contratual até que testes de recuperação medidos permitam fazê-lo; o compromisso contratual é a disponibilidade-alvo de 99,5% ao mês do Anexo A dos Termos de Licença, com créditos por indisponibilidade.

9. CONFORMIDADE E CERTIFICAÇÕES

9.1 A Ergondata atua como operadora dos dados pessoais que os clientes inserem na plataforma, sob o Acordo de Tratamento de Dados Pessoais (Anexo C), em conformidade com a LGPD. Os processos de certificação ISO/IEC 27001 e SOC 2 estão em andamento na data desta versão e não são declarados como obtidos; questionários de segurança são respondidos com base nos controles descritos nesta página e na ficha técnica. **[Teste de intrusão: registrar fornecedor, escopo e data do último teste antes de afirmar a sua realização; até lá, esta página não afirma pentest realizado.]**

10. O QUE A PLATAFORMA NÃO FAZ

a) não executa código no perímetro do cliente; toda execução acontece em infraestrutura da Ergondata;

b) não processa pagamentos nem transações financeiras; valores podem ser registrados como dado informacional de processo, sem integração com meio de pagamento;

c) não realiza transferência de arquivos por SFTP nem carga em lote com terceiros; upload e download acontecem pela própria aplicação;

d) não envia SMS; a comunicação externa ocorre por e-mail e, quando habilitado, por WhatsApp;

e) não oferece implantação dedicada ou single-tenant no padrão; disponibilidade superior a 99,5% e implantação dedicada são objeto de proposta específica.

11. DIVULGAÇÃO RESPONSÁVEL DE VULNERABILIDADES

11.1 Pesquisadores de segurança que identifiquem vulnerabilidade na plataforma ou no site podem reportá-la a **[seguranca@ergondata.ai]**, com descrição, passos de reprodução e impacto estimado. A Ergondata confirma o recebimento em até 2 (dois) dias úteis, mantém o pesquisador informado sobre o tratamento e não adota medidas legais contra quem reportar de boa-fé, sem explorar a falha além do necessário à demonstração, sem acessar ou alterar dados de terceiros e sem divulgar a vulnerabilidade antes da correção.

12. CONTATO

12.1 Segurança da informação: **[seguranca@ergondata.ai]**. Proteção de dados pessoais: privacidade@ergondata.ai. Solicitação da ficha técnica completa sob acordo de confidencialidade: **[formulário]**.

Ergondata · Visão geral de segurança · versão 1.0, setembro de 2026. Documento publicado na seção Legal do site ergondata.ai.
Fontes internas: Plataforma v2.5 (§5, §10) na camada pública do Brand OS v2.16 (§6.6).