# Medidas de Segurança da ProcessMind

Data de vigência: 14 de setembro de 2026

Este documento descreve as medidas técnicas e organizacionais ("TOMs") que a ProcessMind B.V. mantém para proteger a confidencialidade, a integridade e a disponibilidade dos Dados do Cliente. A ProcessMind segue uma abordagem de defesa em profundidade, na qual várias camadas independentes de segurança protegem os Dados do Cliente em todos os níveis — da rede e infraestrutura à identidade, autorização, isolamento de dados, criptografia, monitoramento e desenvolvimento de software. Essas medidas complementam o Adendo de Tratamento de Dados, a Política de Privacidade e a Política de Hospedagem SaaS. A ProcessMind revisa e atualiza essas medidas pelo menos anualmente.

Os Dados do Cliente nunca são vendidos a terceiros, compartilhados com terceiros ou utilizados por terceiros para suas próprias finalidades.

---

### 1. Segurança da Infraestrutura

**1.1 Plataforma de Nuvem.** A ProcessMind está hospedada exclusivamente na Amazon Web Services (AWS) na UE (Frankfurt, Alemanha, `eu-central-1`). A AWS mantém certificações ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 e PCI DSS. Consulte Programas de Conformidade da AWS para obter a lista completa.

**1.2 Arquitetura Serverless.** A lógica da aplicação da ProcessMind é executada no AWS Lambda e em serviços gerenciados pela AWS. A ProcessMind não opera servidores de aplicação de longa duração gerenciados pelo cliente, o que elimina uma grande classe de tarefas de aplicação de patches do sistema operacional e reforço de segurança de servidores.

**1.3 Limites de Rede.** A ProcessMind mantém uma AWS VPC para controles de banco de dados e de rede. O Aurora PostgreSQL é executado em sub-

redes privadas sem saída para a internet, não é acessível publicamente e os logs de fluxo da VPC estão habilitados. A ProcessMind não coloca funções Lambda de aplicação dentro da VPC por padrão. As Lambdas acessam o Aurora por meio da AWS RDS Data API sobre TLS, usando autenticação do IAM e do Secrets Manager.

**1.4 Entrega de Conteúdo e Controles de Borda.** O site voltado aos clientes, a SPA do frontend e o tráfego de recursos públicos são fornecidos por meio do Amazon CloudFront. Todas as distribuições do CloudFront impõem uma política TLS mínima de TLS 1.2 (2021). As distribuições do site e da SPA do frontend também adicionam cabeçalhos de resposta de segurança, incluindo HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, política de referenciador e política de permissões. A distribuição de recursos públicos usa o CloudFront Origin Access Control para manter o bucket de origem privado. O tráfego de API voltado aos clientes é tratado separadamente pelo Amazon API Gateway: o tráfego de solicitação/resposta HTTPS é fornecido por meio de uma HTTP API em um subdomínio de API dedicado, e as conexões de clientes em tempo real são fornecidas por meio de uma API WebSocket separada do API Gateway em um subdomínio WebSocket dedicado.

**1.5 Segregação de Ambientes.** Os ambientes de produção e desenvolvimento usam contas AWS separadas, bancos de dados separados e pilhas de infraestrutura separadas. As credenciais dos desenvolvedores não fornecem acesso aos Dados do Cliente em produção.

---

### 2. Criptografia de Dados

**2.1 Criptografia em Trânsito.** Todos os dados transmitidos entre clientes e serviços da ProcessMind são criptografados usando TLS 1.2 ou superior. Os endpoints voltados aos clientes são expostos por HTTPS. Buckets S3, tópicos SNS e filas SQS criados diretamente pela ProcessMind impõem

acesso somente por SSL. O acesso ao banco de dados por meio da RDS Data API e outras chamadas de serviços da AWS usa HTTPS/TLS.

**2.2 Criptografia em Repouso.** O Aurora PostgreSQL é criptografado em repouso usando chaves AWS KMS gerenciadas pelo cliente, com rotação automática de chaves. Os buckets S3 de dados de clientes e operacionais criados diretamente pela ProcessMind, incluindo buckets de uploads, recursos e logs de acesso, usam chaves KMS gerenciadas pelo cliente. Grupos de logs do CloudWatch, tópicos SNS e filas SQS criados diretamente pela ProcessMind também usam chaves KMS gerenciadas pelo cliente. Os buckets de origem do site e do frontend gerenciados pelo SST usam criptografia do lado do servidor do S3 gerenciada pela AWS (SSE-S3 / AES-256), em vez de chaves KMS gerenciadas pelo cliente.

**2.3 Gerenciamento de Chaves e Segredos.** As chaves de criptografia do banco de dados são gerenciadas centralmente por meio do AWS KMS, e o acesso às chaves é regido por políticas do IAM que seguem os princípios do menor privilégio. As credenciais do banco de dados são armazenadas no AWS Secrets Manager. O segredo mestre do Aurora e o segredo restrito do usuário da aplicação são rotacionados automaticamente a cada trinta (30) dias. Chaves e segredos de produção nunca são armazenados no código-fonte; as credenciais exclusivas de desenvolvimento são isoladas da produção. Alguns recursos de suporte gerenciados pelo AWS/CDK/SST continuam usando criptografia gerenciada pela AWS quando o serviço ou framework não expõe configuração de chave gerenciada pelo cliente.

---

**3. Isolamento e Residência dos Dados**

**3.1 Isolamento de Locatários.** Cada locatário cliente recebe uma instância de banco de dados dedicada e isolada. Os Dados do Cliente nunca são misturados com os dados de outros clientes no nível do banco de dados. Metadados compartilhados (por exemplo, registros de contas, faturamento e mapeamentos de usuário para locatário) são armazenados em um banco de dados separado com vários locatários e

controles de acesso rigorosos. As tabelas compartilhadas com escopo de locatário e organização também são protegidas por políticas de segurança em nível de linha (RLS) do PostgreSQL, aplicadas por meio do contexto do banco de dados com escopo da solicitação.

**3.2 Residência dos Dados.** Todos os Dados do Cliente, incluindo bancos de dados, uploads de arquivos, backups e resultados de consultas, são armazenados exclusivamente na UE (Frankfurt, Alemanha). Quando um suboperador localizado fora do EEE é contratado para uma atividade de tratamento específica (por exemplo, tratamento por modelo de IA ou processamento de pagamentos), a transferência é abrangida por um mecanismo de transferência apropriado, conforme descrito no Adendo de Tratamento de Dados, e o suboperador e seu local de tratamento são listados na Lista de Suboperadores.

**3.3 Retenção e Exclusão de Dados.** Os prazos de retenção e exclusão estão estabelecidos na Seção 6 do Adendo de Tratamento de Dados. Os clientes podem excluir seus dados a qualquer momento por meio da aplicação ou entrando em contato com a ProcessMind. As cópias de backup são removidas quando os períodos de retenção de backup aplicáveis expiram (Seção 7.1).

---

**4. Gerenciamento de Identidade e Acesso**

**4.1 Autenticação.** A ProcessMind oferece suporte a Single Sign-On (SSO) por meio do Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC e LinkedIn OAuth 2.0/OIDC. A ProcessMind atua como parte confiável e não armazena senhas de usuários. A autenticação multifator é imposta pelo provedor de identidade — por exemplo, quando uma organização conecta o Microsoft Entra ID (Azure AD), aplicam-se as próprias políticas de MFA e de acesso dessa organização.

**4.2 Gerenciamento de Sessões.** As sessões do navegador usam JSON Web Tokens (JWT) assinados, transmitidos por cookies seguros e HttpOnly com

os sinalizadores SameSite e Secure. As assinaturas dos tokens são validadas em cada solicitação autenticada.

**4.3 Modelo de Autorização.** A ProcessMind não depende de autorizadores nativos do API Gateway para suas APIs principais da aplicação. A autorização é aplicada em wrappers compartilhados de manipuladores Lambda que validam o estado da sessão e o escopo do locatário antes da execução da lógica de negócios. As rotas públicas são explicitamente incluídas em uma lista de permissões para fluxos não autenticados, webhooks, ingestão de eventos e preflight de CORS. Os endpoints de API externos usam manipuladores de autenticação dedicados. O acesso aos Dados do Cliente é limitado ao contexto do locatário ou da organização autenticado.

**4.4 Menor Privilégio.** Os sistemas internos seguem o princípio do menor privilégio. As funções do IAM têm escopo limitado aos recursos mínimos necessários quando o framework permite um escopo preciso. Algumas funções geradas pelo SST/CDK usam políticas gerenciadas ou inline mais amplas para vinculações e operação em tempo de execução; esses casos são revisados, têm escopo limitado aos recursos quando possível e são registrados como exceções explícitas.

**4.5 Controles de Acesso de Funcionários.** O acesso dos funcionários aos sistemas internos é gerenciado por meio do Active Directory com SSO e MFA obrigatório. O controle de acesso baseado em funções (RBAC) garante que o acesso aos Dados do Cliente seja limitado ao pessoal autorizado com base na necessidade de conhecimento. Os direitos de acesso são revisados periodicamente.

---

**5. Registro, Monitoramento e Auditoria**

**5.1 Registro Centralizado.** O registro de acesso à HTTP API e o registro de acesso ao WebSocket estão habilitados com campos JSON estruturados e são gravados no Amazon CloudWatch Logs, com retenção de uma (1) semana. Esses grupos de logs de acesso são criptografados com uma

chave AWS KMS gerenciada pelo cliente. Os logs da aplicação são centralizados em grupos de logs do Amazon CloudWatch criptografados com uma chave AWS KMS gerenciada pelo cliente e retidos por dez (10) anos. Grupos de logs separados de auditoria e telemetria também são criptografados com uma chave AWS KMS gerenciada pelo cliente e retidos por dez (10) anos. O grupo de exportação de logs do mecanismo Aurora PostgreSQL é retido por uma (1) semana.

**5.2 O que é Registrado e o que Não é Registrado.** A ProcessMind registra eventos de acesso à HTTP API e ao WebSocket, incluindo horário da solicitação, identificadores da solicitação, rota ou caminho, status da resposta, latência, IP de origem e agente do usuário. A ProcessMind também registra eventos de autenticação, caminhos de falha assíncrona e atividades de suporte da aplicação Lambda em grupos de logs centralizados do CloudWatch. Os logs de fluxo da VPC estão habilitados. Atualmente, a ProcessMind não habilita o registro de acesso padrão do CloudFront nas distribuições do site, da SPA do frontend ou de recursos públicos.

**5.3 Monitoramento e Alertas.** Os alarmes e painéis do CloudWatch monitoram a integridade do sistema, as filas de mensagens não entregues e as falhas relevantes para a segurança. As falhas de processamento assíncrono são encaminhadas para filas de mensagens não entregues criptografadas (retenção de quatorze (14) dias; dois (2) dias para as filas de miniaturas e de índice de pesquisa), e os alarmes de DLQ acionam notificações SNS para investigação. Além disso, a ProcessMind usa o Sentry para rastreamento de erros do frontend em tempo real, monitoramento de desempenho e reprodução de sessões. As reproduções de sessões são gravadas somente para sessões nas quais ocorre um erro, e textos, entradas de formulários e mídia são mascarados ou bloqueados nas reproduções. Os dados do Sentry são ingeridos na UE (Frankfurt) e limitados aos Dados de Uso da ProcessMind (erros do navegador, rastreamentos de desempenho, metadados do dispositivo e

gravações de reprodução mascaradas). O Sentry está listado na lista de suboperadores.

**5.4 Proteção de Logs.** Os logs são armazenados em grupos de logs do CloudWatch dedicados e com acesso controlado, e criptografados em repouso. Os logs de produção e desenvolvimento são separados por limites de ambiente e de conta.

---

**6. Validação Automatizada de Controles e Gerenciamento de Vulnerabilidades**

**6.1 O que a ProcessMind Faz.** A ProcessMind executa `cdk-nag` como parte do seu fluxo de síntese e implantação de infraestrutura, usando vários pacotes de regras do setor (incluindo AWS Solutions, NIST 800-53 e PCI DSS). Relatórios por pilha são gerados e revisados como parte do gerenciamento de alterações da infraestrutura. As constatações são classificadas como corrigidas, risco aceito ou melhoria planejada.

**6.2 Como as Exceções são Gerenciadas.** As supressões são registradas em um registro central quando o framework permite, têm escopo limitado às pilhas afetadas e exigem justificativa por escrito; quando uma pilha contém uma supressão inline, ela é documentada junto com essa pilha. Quando uma constatação é corrigida, a supressão correspondente é atualizada ou removida. A ProcessMind não trata a supressão como uma exclusão geral da revisão.

**6.3 O que a ProcessMind Atualmente Não Faz.** A ProcessMind acompanha e revisa exceções materiais aos controles de infraestrutura. As principais são:

- As Lambdas da aplicação não são colocadas dentro da VPC por padrão; elas acessam o Aurora por meio da RDS Data API sobre TLS, com autenticação do IAM e do Secrets Manager
- a WebSocket API e as distribuições estáticas não estão protegidas pelo AWS WAF (as conexões WebSocket usam tokens HMAC de

curta duração; as restrições geográficas relacionadas a pagamentos são aplicadas no sistema de pagamentos), e as distribuições estáticas não têm registro de acesso padrão do CloudFront

- a recuperação do banco de dados depende dos backups automatizados e da recuperação point-in-time do Aurora, e não de um plano separado do AWS Backup ou do Aurora Enhanced Monitoring
- não há replicação S3 entre regiões nem S3 Object Lock para buckets mutáveis
- alguns recursos de suporte gerenciados pelo AWS/CDK/SST usam criptografia gerenciada pela AWS ou políticas IAM geradas mais amplas quando o serviço não oferece uma alternativa controlada pelo cliente

O registro completo de supressões é mantido junto com o código de infraestrutura e está disponível mediante solicitação. O uso de `cdk-nag` pacotes de regras constitui validação de controles de engenharia, e não uma certificação externa, opinião de auditoria ou atestado legal de conformidade com HIPAA, NIST ou PCI DSS.

**6.4 Gerenciamento de Dependências.** As dependências de software são monitoradas continuamente quanto a vulnerabilidades conhecidas. Vulnerabilidades críticas e de alta gravidade são corrigidas com uma meta de sete (7) dias. As dependências são atualizadas em um ciclo regular.

**6.5 Ciclo de Vida de Desenvolvimento Seguro de Software (SDLC).** A ProcessMind segue uma abordagem de defesa em profundidade para o desenvolvimento de software. Toda alteração na produção deve passar por várias camadas independentes de validação automatizada antes da implantação:

- **Análise estática e segurança de tipos:** o modo estrito do TypeScript e o ESLint impõem a correção de tipos, a segurança contra valores

nulos e padrões de codificação relevantes para a segurança em tempo de compilação.

- **Revisão de código assistida por IA:** a análise assistida por IA fornece uma perspectiva adicional de revisão sobre pull requests para identificar riscos de segurança, erros lógicos e desvios de convenções, complementando os testes automatizados.
- **Testes unitários e de integração:** uma suíte abrangente de testes Vitest valida a lógica de negócios, os padrões de acesso a dados, o comportamento da API e o tratamento de erros em relação a recursos AWS ativos no ambiente de desenvolvimento.
- **Testes de ponta a ponta:** testes de navegador baseados em Playwright verificam fluxos de trabalho críticos dos usuários, incluindo autenticação, upload de dados, modelagem de processos, simulação e isolamento entre múltiplos locatários.
- **Verificação de conformidade da infraestrutura:** `cdk-nag` valida a infraestrutura como código em relação a várias estruturas de conformidade a cada alteração.
- **Verificação de vulnerabilidades das dependências:** auditorias automatizadas de dependências impedem que vulnerabilidades críticas e de alta gravidade conhecidas cheguem à produção.

A revisão humana concentra-se na arquitetura, nos limites de segurança e nas decisões em nível de projeto, e não na inspeção do código linha a linha. Quando houver alterações estruturais, sensíveis à segurança ou de infraestrutura, é necessária aprovação humana explícita além da validação automatizada.

Todas as camadas de validação são impostas por meio de CI como gates obrigatórios de merge para alterações na branch principal. Correções emergenciais em produção podem ignorar o gate de CI, mas devem ser seguidas por uma execução completa do pipeline e uma revisão pós-incidente no prazo de vinte e quatro (24) horas.

---

### 7. Backup e Recuperação de Desastres

**7.1 Backups Automatizados.** O Amazon Aurora realiza backups contínuos e automatizados, com período de retenção de sete (7) dias. Os backups são criptografados usando as mesmas chaves KMS gerenciadas pelo cliente que os bancos de dados de origem.

**7.2 Recuperação Point-in-Time.** O Aurora oferece recuperação point-in-time para qualquer segundo dentro da janela de retenção de backup, permitindo a restauração rápida em caso de corrupção de dados ou exclusão acidental.

**7.3 Durabilidade e Versionamento do S3.** Os uploads de arquivos e artefatos operacionais são armazenados no Amazon S3, que oferece durabilidade de 99,999999999% (11 noves). O versionamento está habilitado no bucket de uploads e nos buckets de recursos para permitir recuperação e reversões. Os buckets de implantação do site e do frontend são artefatos de build reproduzíveis e não são tratados como um sistema de backup. Atualmente, a ProcessMind não habilita a replicação S3 entre regiões.

**7.4 Continuidade de Negócios.** Os procedimentos de recuperação de desastres são documentados e testados periodicamente. Um resumo está disponível no documento Recuperação de Desastres, Continuidade de Negócios e Resposta a Incidentes. A arquitetura depende de serviços gerenciados pela AWS dentro da `eu-central-1` região, que a AWS opera em várias Zonas de Disponibilidade; o cluster Aurora atualmente executa uma única instância de gravação, portanto a recuperação do banco de dados depende de backups automatizados e recuperação point-in-time, e não de uma instância de espera na região. Os backups do Aurora, a durabilidade do S3, as filas de mensagens não entregues e os ativos estáticos reconstruídos a partir da origem fazem parte da estratégia de recuperação.

---

**8. Resposta a Incidentes**

**8.1 Notificação de Incidentes.** No caso de um Incidente de Segurança (conforme definido no DPA), a ProcessMind notificará os clientes afetados sem demora indevida e, quando viável, no prazo de setenta e duas (72) horas após tomar conhecimento do incidente.

**8.2 Tratamento de Incidentes.** A ProcessMind mantém procedimentos documentados de resposta a incidentes que abrangem identificação, contenção, erradicação, recuperação e revisão pós-incidente. Um resumo está disponível no documento Recuperação de Desastres, Continuidade de Negócios e Resposta a Incidentes. As lições aprendidas com os incidentes são incorporadas aos controles e processos de segurança.

**8.3 Comunicação.** As notificações de incidentes incluem a natureza e o escopo do incidente, as categorias de dados afetadas, as medidas tomadas para conter o incidente e as ações recomendadas ao cliente.

---

**9. Medidas Organizacionais**

**9.1. Gestão da Segurança da Informação.** A ProcessMind mantém um sistema de gestão da segurança da informação alinhado aos princípios da ISO 27001. A ProcessMind selecionou seu caminho de certificação para a certificação ISO 27001 e o atestado SOC 2 Type II; o processo formal de certificação ainda não foi iniciado.

**9.2 Conscientização sobre Segurança.** Todo o pessoal com acesso aos Dados do Cliente recebe treinamento de conscientização sobre segurança. As melhores práticas de segurança estão incorporadas à integração, aos fluxos de desenvolvimento e aos procedimentos operacionais.

**9.3 Gestão de Fornecedores e Subprocessadores.** Os subprocessadores estão contratualmente vinculados a padrões de proteção de dados equivalentes aos descritos neste documento. A ProcessMind mantém uma lista pública de subprocessadores e fornece aviso prévio de pelo menos

trinta (30) dias antes de contratar um novo subprocessador. Os subprocessadores são revisados anualmente quanto à conformidade.

**9.4 Confidencialidade.** Todo o pessoal autorizado a processar Dados do Cliente está vinculado a obrigações de confidencialidade por escrito.

---

### 10. Conformidade e Certificações

| Estrutura / Norma | Status |
|---|---|
| GDPR (Regulamento Geral sobre a Proteção de Dados da UE) | Em conformidade |
| Residência de Dados da UE (Frankfurt, Alemanha) | Aplicada |
| Certificações da Infraestrutura AWS (ISO 27001, SOC 2, PCI DSS) | Herdadas da AWS |
| ISO 27001 (ProcessMind) | Planejada — caminho de certificação selecionado; processo formal ainda não iniciado |
| SOC 2 Type II (ProcessMind) | Planejada — caminho de certificação selecionado; processo formal ainda não iniciado |
| Validação automatizada de controles de infraestrutura (`cdk-nag` em AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless) | Implementada como validação de controles de engenharia, não como certificação |
| Cláusulas Contratuais Padrão (SCCs) para transferências internacionais | Implementadas (consulte o DPA) |

| Estrutura / Norma | Status |
| --- | --- |
| Aditivo de Processamento de Dados (DPA) | Disponível publicamente |

O uso de `cdk-nag` pacotes de regras não significa que a ProcessMind seja formalmente certificada ou auditada de forma independente em relação à HIPAA, ao NIST ou à PCI DSS. Esses pacotes de regras são usados como salvaguardas de engenharia para validar o projeto da infraestrutura e acompanhar explicitamente as lacunas.

Para dúvidas relacionadas à segurança, conformidade ou para solicitar documentação, como relatórios de auditoria ou questionários de segurança preenchidos, entre em contato com **support@processmind.com**.