Recuperação de Desastres, Continuidade de Negócios e Resposta a Incidentes da ProcessMind

Data de vigência: 14 de setembro de 2026

Este documento fornece um resumo de alto nível dos procedimentos da ProcessMind B.V. para recuperação de desastres ("DR"), continuidade de negócios ("BCP") e resposta a incidentes de segurança para seu serviço de nuvem. Ele complementa as Medidas de Segurança, a Política de Hospedagem SaaS, o Acordo de Nível de Serviço e o Aditivo de Processamento de Dados.

Ele explica nossa abordagem atual e não cria objetivos contratuais separados de tempo de recuperação, objetivos de ponto de recuperação, garantias de durabilidade de dados, prazos de notificação, níveis de serviço ou padrões de responsabilidade além do que estiver expressamente estabelecido no contrato, DPA ou SLA aplicável.

---

1. Objetivos e Escopo

A ProcessMind mantém estes procedimentos para:

- proteger a confidencialidade, integridade e disponibilidade dos Dados do Cliente durante um evento disruptivo
- restaurar componentes críticos do serviço de produção após falhas em sistemas controlados pela ProcessMind
- dar continuidade ao gerenciamento de incidentes, à comunicação com clientes e à tomada de decisões operacionais durante interrupções do serviço
- recuperar-se de falhas de infraestrutura, implantação, aplicação ou camada de dados usando procedimentos documentados e definições de infraestrutura controladas por código-fonte
- identificar e avaliar Incidentes de Segurança, conter ameaças, eliminar causas-raiz, recuperar sistemas afetados, comunicar conforme necessário e registrar as lições aprendidas

Estes procedimentos se aplicam ao serviço de nuvem de produção da ProcessMind e a eventos de segurança que envolvam subprocessadores ou serviços de nuvem na medida em que afetem o Serviço e estejam dentro da capacidade razoável da ProcessMind de investigar e gerenciar. Os ambientes de desenvolvimento e teste são segregados e não são tratados como alvos de recuperação para compromissos de produção voltados aos clientes.

---

2. Estratégia de Resiliência

2.1 Projeto Regional. Os serviços de produção são hospedados na AWS EU (Frankfurt, Alemanha, `eu-central-1`). A arquitetura depende de serviços gerenciados da AWS nessa região, que a AWS opera em várias Availability Zones. O cluster Aurora atualmente executa uma única instância de gravação, portanto a recuperação do banco de dados depende de backups automatizados e recuperação pontual, e não de um standby na região. A ProcessMind atualmente não opera uma segunda região ativa de dados de clientes.

2.2 Serviços Gerenciados e Serverless. A ProcessMind depende de AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS e Amazon CloudWatch. Isso reduz a dependência de servidores de longa duração gerenciados pelo cliente e permite a recuperação por reconstrução a partir do código-fonte para componentes de aplicação e estáticos.

2.3 Separação de Ambientes. Os ambientes de produção e desenvolvimento operam em contas AWS separadas, com bancos de dados e stacks de infraestrutura separados. Isso reduz o risco de que atividades de desenvolvimento afetem as operações de recuperação da produção.

2.4 Monitoramento e Detecção. Alarmes do CloudWatch, painéis, alertas de filas de mensagens não entregues, registro centralizado e monitoramento sintético do serviço apoiam a detecção, triagem e

escalonamento de incidentes. Incidentes potenciais também podem ser identificados por meio de solicitações de suporte, relatos de funcionários, notificações de fornecedores ou outros gatilhos de investigação.

---

3. Prioridades de Recuperação

Durante um incidente grave, as prioridades de recuperação da ProcessMind são geralmente:

1. Proteger a integridade dos dados dos clientes e impedir danos adicionais.
2. Conter o incidente e estabilizar os sistemas afetados.
3. Restaurar os caminhos essenciais de acesso à produção e os fluxos de trabalho críticos.
4. Validar o comportamento do serviço, a integridade dos dados e o monitoramento antes de declarar a recuperação concluída.
5. Comunicar atualizações de status, impacto para os clientes e ações de acompanhamento.

A sequência exata pode variar dependendo da natureza do incidente, inclusive se ele afetar a integridade dos dados, o acesso dos clientes, o processamento assíncrono ou a infraestrutura de suporte.

---

4. Procedimentos de Recuperação de Desastres

4.1 Declaração e Coordenação do Incidente. Interrupções materiais do serviço e incidentes de segurança são submetidos à triagem por meio de procedimentos de resposta a incidentes. A ProcessMind designa um responsável pelo incidente, limita a participação na resposta a pessoal autorizado, avalia a gravidade e o escopo, coordena os responsáveis técnicos e acompanha as ações de recuperação até que o incidente seja resolvido ou rebaixado.

4.2 Contenção. A ProcessMind emprega esforços comercialmente razoáveis para interromper ou reduzir o impacto contínuo antes do início

de uma restauração mais ampla. Dependendo do modo de falha, as ações de contenção podem incluir reverter alterações recentes, desativar caminhos afetados, isolar componentes com mau funcionamento, pausar o processamento em segundo plano enquanto são realizadas verificações de integridade, revogar ou alternar credenciais ou bloquear atividades abusivas.

4.3 Erradicação. Depois que o impacto imediato é estabilizado, a ProcessMind trabalha para remover a causa-raiz ou a condição contribuinte. Isso pode incluir aplicar correções de código ou configuração, remover artefatos maliciosos, alternar segredos, restaurar configurações confiáveis ou fechar caminhos de acesso expostos.

4.4 Recuperação do Banco de Dados. O Aurora PostgreSQL realiza backups automatizados contínuos com uma janela de retenção de sete (7) dias e oferece recuperação pontual. Se uma falha no nível do banco de dados, um evento de corrupção ou uma alteração destrutiva acidental exigir restauração, a ProcessMind poderá restaurar a partir do backup adequado mais recente ou até um ponto selecionado no tempo, validar o ambiente restaurado e direcionar o tráfego da aplicação de volta ao caminho do banco de dados recuperado.

4.5 Recuperação de Objetos e Artefatos. Os uploads de arquivos dos clientes e os artefatos operacionais são armazenados no Amazon S3. O versionamento está habilitado no bucket de uploads e nos buckets de recursos para apoiar a recuperação de cenários de exclusão ou substituição acidental. Os buckets de implantação do site e do frontend são tratados como artefatos reproduzíveis e podem ser reconstruídos a partir do código-fonte, em vez de restaurados como backups.

4.6 Recuperação de Cargas de Trabalho Assíncronas. Os caminhos de processamento assíncrono usam filas de mensagens não entregues para reter eventos com falha para investigação. A recuperação pode incluir tentar novamente mensagens com falha, executar novamente a lógica de processamento ou reproduzir o trabalho quando o fluxo de trabalho subjacente permitir o reprocessamento seguro.

4.7 Reconstrução da Aplicação e da Infraestrutura. A infraestrutura é gerenciada por meio de definições de infraestrutura como código controladas por código-fonte. Se a infraestrutura da aplicação ou os ativos estáticos precisarem ser recriados, a ProcessMind poderá reconstruir e reimplantar os componentes afetados a partir de definições e artefatos de compilação controlados por versão.

4.8 Validação Antes do Retorno ao Serviço. Antes de encerrar um incidente, a ProcessMind valida a integridade do serviço usando o monitoramento, os logs, as verificações sintéticas e a verificação funcional direcionada disponíveis, e restaura a funcionalidade afetada usando procedimentos validados de implantação, recuperação e infraestrutura. Uma análise adicional pode ser realizada quando o incidente envolver restauração de dados ou risco à integridade dos dados.

---

5. Medidas de Continuidade de Negócios

5.1 Continuidade Operacional. A ProcessMind mantém procedimentos operacionais documentados para que o tratamento de incidentes, o recebimento de solicitações de suporte, a resposta de engenharia e a tomada de decisões possam continuar durante eventos disruptivos.

5.2 Comunicações. Para incidentes materiais de produção, a ProcessMind emprega esforços comercialmente razoáveis para fornecer atualizações por meio dos canais de suporte ao cliente e, quando apropriado, da página pública de status em processmind.com/status.

5.3 Gerenciamento Controlado de Alterações. Um ciclo de vida de desenvolvimento de software com defesa em profundidade, múltiplas camadas independentes de validação automatizada, implantações controladas, monitoramento centralizado e análise pós-incidente é usado para reduzir interrupções evitáveis e melhorar a continuidade ao longo do tempo.

5.4 Segurança Durante a Recuperação. As ações de recuperação são realizadas sujeitas aos mesmos princípios gerais de segurança aplicáveis durante as operações normais, incluindo acesso com privilégio mínimo, registro das atividades operacionais quando disponível e acesso controlado aos sistemas e dados de produção.

---

6. Resumo de Backup e Proteção de Dados

6.1 Backups do Banco de Dados. Os backups automatizados do Aurora são criptografados e retidos por sete (7) dias, com recuperação pontual disponível dentro dessa janela de retenção.

6.2 Proteções do S3. O Amazon S3 oferece alta durabilidade para objetos armazenados. Os buckets de dados de clientes mutáveis dependem da durabilidade e do versionamento na região primária. Atualmente, o ProcessMind não habilita a replicação do S3 entre regiões para esses buckets.

6.3 Registros e diagnósticos. Registros, alarmes e telemetria centralizados apoiam a investigação de falhas e a validação da recuperação. Esses mecanismos apoiam as operações de continuidade, mas não são apresentados, por si só, como um produto de backup separado.

---

7. Identificação e triagem de incidentes

7.1 Avaliação inicial. Os eventos comunicados são submetidos a triagem para determinar se atendem à definição de um Incidente de Segurança, quais sistemas ou dados podem ser afetados, o provável escopo e a gravidade, e se é necessário realizar contenção imediata. A preservação de evidências é realizada de maneira apropriada à natureza do incidente e aos sistemas envolvidos.

7.2 Plantão e escalonamento. O ProcessMind mantém cobertura de plantão para incidentes de produção, incluindo cobertura 24 horas por dia, 7 dias por semana para incidentes Críticos (conforme definidos no Acordo

de Nível de Serviço), para que os incidentes possam ser reconhecidos e submetidos a triagem a qualquer momento.

7.3 Documentação. O ProcessMind documenta as conclusões relevantes da investigação, as ações de resposta e as decisões de recuperação, para que a linha do tempo do incidente e as ações corretivas resultantes possam ser analisadas após o evento.

---

8. Comunicações e notificações

8.1 Comunicação interna. O ProcessMind coordena os responsáveis pela resposta, os tomadores de decisão e os canais de suporte para que a resposta técnica e a comunicação com os clientes permaneçam alinhadas durante todo o ciclo de vida do incidente.

8.2 Notificação aos clientes. No caso de um Incidente de Segurança que exija notificação nos termos do DPA ou da legislação aplicável, o ProcessMind notifica os clientes afetados sem demora indevida e, quando viável, no prazo de setenta e duas (72) horas a contar do momento em que tomar conhecimento do incidente. As notificações geralmente incluem a natureza e o escopo do incidente, as categorias de dados afetadas, se conhecidas, as medidas tomadas para conter e remediar o incidente e as ações recomendadas aos clientes, quando relevantes.

8.3 Atualizações contínuas. Quando o incidente permanece ativo ou fatos relevantes são alterados, o ProcessMind fornece atualizações de acompanhamento à medida que informações adicionais verificadas se tornam disponíveis. Para interrupções mais amplas do serviço de produção, o ProcessMind também pode utilizar canais de suporte ao cliente e, quando apropriado, a página pública de status em processmind.com/status.

---

9. Testes, revisão e manutenção

O ProcessMind revisa estes procedimentos pelo menos anualmente e após incidentes relevantes ou alterações arquitetônicas significativas, testa periodicamente elementos pertinentes da abordagem de resposta e recuperação (como restauração de backups, reconstrução de implantações, monitoramento, alertas e comunicações sobre incidentes) e incorpora as lições aprendidas aos seus procedimentos de segurança, confiabilidade e continuidade.

---

10. Limitações e limites contratuais

Este documento é um resumo de alto nível e não descreve detalhadamente todos os runbooks internos, caminhos de escalonamento, métodos de investigação ou etapas de tratamento de evidências. Ele não obriga o ProcessMind a adotar um projeto separado de failover entre regiões, retenção de armazenamento imutável para todos os buckets mutáveis ou garantias independentes de RTO/RPO além do que estiver expressamente estabelecido no contrato ou pedido aplicável.

Se houver qualquer conflito entre este documento e o Contrato do Cliente, o Adendo de Processamento de Dados, o Acordo de Nível de Serviço ou a legislação obrigatória aplicável, essas fontes prevalecerão.