Recuperación ante desastres, continuidad del negocio y respuesta a incidentes de ProcessMind

Fecha de entrada en vigor: 14 de septiembre de 2026

Este documento proporciona un resumen de alto nivel de los procedimientos de recuperación ante desastres («DR»), continuidad del negocio («BCP») y respuesta a incidentes de seguridad de ProcessMind B.V. para su servicio en la nube. Complementa las Medidas de seguridad, la Política de alojamiento SaaS, el Acuerdo de nivel de servicio y el Anexo de tratamiento de datos.

Explica nuestro enfoque actual y no crea objetivos contractuales independientes de tiempo de recuperación, objetivos de punto de recuperación, garantías de durabilidad de los datos, plazos de notificación, niveles de servicio ni estándares de responsabilidad más allá de lo expresamente establecido en el acuerdo aplicable, el DPA o el SLA.

---

1. Objetivos y ámbito de aplicación

ProcessMind mantiene estos procedimientos para:

- proteger la confidencialidad, integridad y disponibilidad de los Datos del Cliente durante un evento disruptivo
- restaurar los componentes críticos del servicio de producción después de fallos en sistemas controlados por ProcessMind
- continuar la gestión de incidentes, la comunicación con los clientes y la toma de decisiones operativas durante interrupciones del servicio
- recuperarse de fallos de infraestructura, implementación, aplicación o capa de datos mediante procedimientos documentados y definiciones de infraestructura bajo control de versiones
- identificar y evaluar Incidentes de Seguridad, contener las amenazas, erradicar las causas raíz, recuperar los sistemas

afectados, comunicar según sea necesario y documentar las lecciones aprendidas

Estos procedimientos se aplican al servicio en la nube de producción de ProcessMind y a los eventos de seguridad que involucren a subencargados o servicios en la nube en la medida en que afecten al Servicio y estén dentro de la capacidad razonable de ProcessMind para investigarlos y gestionarlos. Los entornos de desarrollo y prueba están segregados y no se consideran objetivos de recuperación para compromisos de producción orientados al cliente.

---

2. Estrategia de resiliencia

2.1 Diseño regional. Los servicios de producción están alojados en AWS EU (Fráncfort, Alemania, `eu-central-1`). La arquitectura depende de servicios gestionados de AWS dentro de esa región, que AWS opera en varias zonas de disponibilidad. El clúster de Aurora funciona actualmente con una única instancia de escritura, por lo que la recuperación de la base de datos depende de respaldos automatizados y de la recuperación a un momento dado, en lugar de una instancia en espera dentro de la región. Actualmente, ProcessMind no opera una segunda región activa para los datos de los clientes.

2.2 Servicios gestionados y sin servidor. ProcessMind depende de AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS y Amazon CloudWatch. Esto reduce la dependencia de servidores de larga duración gestionados por los clientes y permite la recuperación mediante la reconstrucción desde el código fuente para los componentes de la aplicación y estáticos.

2.3 Separación de entornos. Los entornos de producción y desarrollo funcionan en cuentas de AWS separadas, con bases de datos y pilas de infraestructura independientes. Esto reduce el riesgo de que la actividad de desarrollo afecte a las operaciones de recuperación de producción.

2.4 Supervisión y detección. Las alarmas y los Dashboard de CloudWatch, las alertas de las colas de mensajes no entregados, el registro centralizado y la supervisión sintética de los servicios contribuyen a la detección, clasificación y escalada de incidentes. Los posibles incidentes también pueden identificarse mediante la recepción de solicitudes de asistencia, los informes de empleados, las notificaciones de proveedores u otros factores desencadenantes de investigaciones.

---

3. Prioridades de recuperación

Durante un incidente grave, las prioridades de recuperación de ProcessMind son, por lo general:

1. Proteger la integridad de los datos de los clientes y evitar daños adicionales.
2. Contener el incidente y estabilizar los sistemas afectados.
3. Restaurar las vías de acceso principales a producción y los flujos de trabajo críticos.
4. Validar el comportamiento del servicio, la integridad de los datos y la supervisión antes de declarar completa la recuperación.
5. Comunicar actualizaciones sobre el estado, el impacto en los clientes y las medidas de seguimiento.

La secuencia exacta puede variar en función de la naturaleza del incidente, incluido si afecta a la integridad de los datos, al acceso de los clientes, al procesamiento asíncrono o a la infraestructura de soporte.

---

4. Procedimientos de recuperación ante desastres

4.1 Declaración y coordinación del incidente. Las interrupciones sustanciales del servicio y los incidentes de seguridad se clasifican mediante procedimientos de respuesta a incidentes. ProcessMind designa a un responsable del incidente, limita la participación en la respuesta al personal autorizado, evalúa la gravedad y el alcance, coordina a los

responsables técnicos y realiza el seguimiento de las medidas de recuperación hasta que el incidente se resuelve o se reduce su nivel.

4.2 Contención. ProcessMind realiza esfuerzos comercialmente razonables para detener o reducir el impacto en curso antes de iniciar una restauración más amplia. Dependiendo del modo de fallo, las medidas de contención pueden incluir revertir cambios recientes, deshabilitar vías afectadas, aislar componentes que funcionen incorrectamente, pausar el procesamiento en segundo plano mientras se realizan comprobaciones de integridad, revocar o rotar credenciales, o bloquear actividades abusivas.

4.3 Erradicación. Una vez estabilizado el impacto inmediato, ProcessMind trabaja para eliminar la causa raíz o la condición contribuyente. Esto puede incluir aplicar correcciones de código o configuración, eliminar artefactos maliciosos, rotar secretos, restaurar una configuración fiable o cerrar vías de acceso expuestas.

4.4 Recuperación de la base de datos. Aurora PostgreSQL realiza respaldos automatizados continuos con un periodo de conservación de siete (7) días y admite la recuperación a un momento dado. Si un fallo a nivel de base de datos, un evento de corrupción o un cambio destructivo accidental requiere una restauración, ProcessMind puede restaurar desde el respaldo adecuado más reciente o hasta un momento seleccionado, validar el entorno restaurado y devolver el tráfico de la aplicación a la vía de la base de datos recuperada.

4.5 Recuperación de objetos y artefactos. Las cargas de archivos de los clientes y los artefactos operativos se almacenan en Amazon S3. El control de versiones está habilitado en el bucket de cargas y en los buckets de recursos para permitir la recuperación en casos de eliminación o sobrescritura accidentales. Los buckets de implementación del sitio web y del frontend se consideran artefactos reproducibles y pueden reconstruirse desde el código fuente en lugar de restaurarse como respaldos.

4.6 Recuperación de cargas de trabajo asíncronas. Las vías de procesamiento asíncrono utilizan colas de mensajes no entregados para conservar los eventos fallidos para su investigación. La recuperación puede incluir reintentar mensajes fallidos, volver a ejecutar la lógica de procesamiento o reproducir el trabajo cuando el flujo de trabajo subyacente permita un reprocesamiento seguro.

4.7 Reconstrucción de la aplicación y la infraestructura. La infraestructura se gestiona mediante definiciones de infraestructura como código bajo control de versiones. Si es necesario recrear la infraestructura de la aplicación o los activos estáticos, ProcessMind puede reconstruir y volver a implementar los componentes afectados a partir de definiciones bajo control de versiones y artefactos de compilación.

4.8 Validación antes de volver a prestar el servicio. Antes de cerrar un incidente, ProcessMind valida el estado del servicio mediante la supervisión, los registros, las comprobaciones sintéticas y la verificación funcional específica disponibles, y restaura la funcionalidad afectada utilizando procedimientos validados de implementación, recuperación e infraestructura. Puede realizarse una revisión adicional cuando el incidente haya implicado la restauración de datos o un riesgo para la integridad de los datos.

---

5. Medidas de continuidad del negocio

5.1 Continuidad operativa. ProcessMind mantiene procedimientos operativos documentados para que la gestión de incidentes, la recepción de solicitudes de soporte de clientes, la respuesta de ingeniería y la toma de decisiones puedan continuar durante eventos disruptivos.

5.2 Comunicaciones. Para incidentes sustanciales de producción, ProcessMind realiza esfuerzos comercialmente razonables para proporcionar actualizaciones a través de los canales de soporte al cliente y, cuando corresponda, mediante la página pública de estado en processmind.com/status.

5.3 Gestión controlada de cambios. Se utiliza un ciclo de vida de desarrollo de software de defensa en profundidad, con múltiples capas independientes de validación automatizada, implementaciones controladas, supervisión centralizada y revisión posterior a los incidentes, para reducir las interrupciones evitables y mejorar la continuidad con el tiempo.

5.4 Seguridad durante la recuperación. Las medidas de recuperación se llevan a cabo sujetas a los mismos principios generales de seguridad aplicables durante las operaciones normales, incluido el acceso con privilegios mínimos, el registro de la actividad operativa cuando esté disponible y el acceso controlado a los sistemas y datos de producción.

---

6. Resumen de respaldos y protección de datos

6.1 Respaldos de la base de datos. Los respaldos automatizados de Aurora están cifrados y se conservan durante siete (7) días; la recuperación a un momento dado está disponible dentro de dicho periodo de conservación.

6.2 Protecciones de S3. Amazon S3 proporciona una alta durabilidad para los objetos almacenados. Los buckets de datos de clientes mutables dependen de la durabilidad y el versionado dentro de la región principal. Actualmente, ProcessMind no habilita la replicación de S3 entre regiones para dichos buckets.

6.3 Registros y diagnósticos. Los registros, las alarmas y la telemetría centralizados respaldan la investigación de fallos y la validación de la recuperación. Estos mecanismos respaldan las operaciones de continuidad, pero no se presentan por sí mismos como un producto de copia de seguridad independiente.

---

7. Identificación y triaje de incidentes

7.1 Evaluación inicial. Los eventos notificados se someten a triaje para determinar si cumplen la definición de Incidente de Seguridad, qué

sistemas o datos podrían verse afectados, el alcance y la gravedad probables, y si se requiere una contención inmediata. La preservación de pruebas se lleva a cabo de manera adecuada a la naturaleza del incidente y a los sistemas involucrados.

7.2 Guardia y escalamiento. ProcessMind mantiene cobertura de guardia para incidentes de producción, incluida cobertura 24x7 para incidentes Críticos (según se definen en el Acuerdo de Nivel de Servicio), de modo que los incidentes puedan reconocerse y someterse a triaje en cualquier momento.

7.3 Documentación. ProcessMind documenta las conclusiones materiales de la investigación, las medidas de respuesta y las decisiones de recuperación, de modo que la cronología del incidente y las medidas correctivas resultantes puedan revisarse después del evento.

---

8. Comunicaciones y notificación

8.1 Comunicación interna. ProcessMind coordina a los responsables de la respuesta, los responsables de la toma de decisiones y los canales de soporte para que la respuesta técnica y la comunicación con los clientes permanezcan alineadas durante todo el ciclo de vida del incidente.

8.2 Notificación a los clientes. En caso de un Incidente de Seguridad que requiera notificación conforme al DPA o a la legislación aplicable, ProcessMind notifica a los clientes afectados sin demora indebida y, cuando sea factible, dentro de las setenta y dos (72) horas siguientes a haber tenido conocimiento del incidente. Las notificaciones generalmente incluyen la naturaleza y el alcance del incidente, las categorías de datos afectadas, si se conocen, las medidas adoptadas para contener y remediar el incidente, y las medidas recomendadas para los clientes cuando sean pertinentes.

8.3 Actualizaciones continuas. Cuando el incidente siga activo o cambien los hechos materiales, ProcessMind proporciona actualizaciones de

seguimiento a medida que se disponga de información adicional verificada. Para interrupciones más amplias del servicio de producción, ProcessMind también puede utilizar los canales de soporte al cliente y, cuando proceda, la página pública de estado en processmind.com/status.

---

9. Pruebas, revisión y mantenimiento

ProcessMind revisa estos procedimientos al menos una vez al año y después de incidentes materiales o cambios arquitectónicos significativos, prueba periódicamente elementos pertinentes del enfoque de respuesta y recuperación (como la restauración de copias de seguridad, la reconstrucción de implementaciones, la supervisión, las alertas y las comunicaciones sobre incidentes), e incorpora las lecciones aprendidas a sus procedimientos de seguridad, fiabilidad y continuidad.

---

10. Limitaciones y límites contractuales

Este documento es un resumen de alto nivel y no describe en detalle operativo cada runbook interno, vía de escalamiento, método de investigación o paso de gestión de pruebas. No compromete a ProcessMind con un diseño independiente de conmutación por error entre regiones, una retención de almacenamiento inmutable para todos los buckets mutables ni garantías independientes de RTO/RPO más allá de lo expresamente establecido en el acuerdo u orden aplicable.

Si existe algún conflicto entre este documento y el Acuerdo del Cliente, el Anexo de Tratamiento de Datos, el Acuerdo de Nivel de Servicio o la legislación imperativa aplicables, prevalecerán dichas fuentes.