Ripristino di emergenza, continuità operativa e risposta agli incidenti di ProcessMind

Data di entrata in vigore: 14 settembre 2026

Il presente documento fornisce una sintesi di alto livello delle procedure di ProcessMind B.V. relative al ripristino di emergenza ("DR"), alla continuità operativa ("BCP") e alla risposta agli incidenti di sicurezza per il proprio servizio cloud. Integra le Misure di sicurezza, la Politica di hosting SaaS, il Service Level Agreement e l'Addendum sul trattamento dei dati.

Spiega il nostro approccio attuale e non crea obiettivi contrattuali separati relativi ai tempi di ripristino, obiettivi relativi ai punti di ripristino, garanzie sulla durabilità dei dati, termini per le notifiche, livelli di servizio o standard di responsabilità oltre a quanto espressamente previsto dall'accordo applicabile, dal DPA o dallo SLA.

---

1. Obiettivi e ambito di applicazione

ProcessMind mantiene queste procedure per:

- proteggere la riservatezza, l'integrità e la disponibilità dei Dati del Cliente durante un evento di interruzione
- ripristinare i componenti critici del servizio di produzione dopo guasti nei sistemi controllati da ProcessMind
- proseguire la gestione degli incidenti, le comunicazioni con i clienti e il processo decisionale operativo durante le interruzioni del servizio
- ripristinare l'infrastruttura, la distribuzione, l'applicazione o i livelli di dati dopo guasti, utilizzando procedure documentate e definizioni dell'infrastruttura sottoposte a controllo del codice sorgente
- identificare e valutare gli Incidenti di sicurezza, contenere le minacce, eliminare le cause alla radice, ripristinare i sistemi interessati, comunicare come richiesto e acquisire gli insegnamenti tratti

Queste procedure si applicano al servizio cloud di produzione di ProcessMind e agli eventi di sicurezza che coinvolgono sub-responsabili o servizi cloud nella misura in cui incidono sul Service e rientrano nella ragionevole capacità di ProcessMind di indagare e gestire tali eventi. Gli ambienti di sviluppo e test sono segregati e non sono considerati obiettivi di ripristino per gli impegni relativi alla produzione rivolta ai clienti.

---

2. Strategia di resilienza

2.1 Progettazione regionale. I servizi di produzione sono ospitati in AWS EU (Francoforte, Germania, `eu-central-1`). L'architettura si basa sui servizi gestiti AWS all'interno di tale regione, che AWS gestisce attraverso più Availability Zones. Il cluster Aurora attualmente esegue una singola istanza writer, pertanto il ripristino del database si basa su backup automatizzati e sul ripristino point-in-time anziché su uno standby nella regione. Attualmente ProcessMind non gestisce una seconda regione attiva per i dati dei clienti.

2.2 Servizi gestiti e serverless. ProcessMind si basa su AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS e Amazon CloudWatch. Ciò riduce la dipendenza da server di lunga durata gestiti dai clienti e supporta il ripristino mediante ricostruzione dal codice sorgente per i componenti applicativi e statici.

2.3 Separazione degli ambienti. Gli ambienti di produzione e sviluppo operano in account AWS separati, con database e stack infrastrutturali separati. Ciò riduce il rischio che le attività di sviluppo incidano sulle operazioni di ripristino della produzione.

2.4 Monitoraggio e rilevamento. Gli allarmi e i dashboard CloudWatch, gli avvisi delle dead-letter queue, la registrazione centralizzata e il monitoraggio sintetico dei servizi supportano il rilevamento, il triage e l'escalation degli incidenti. I potenziali incidenti possono inoltre essere

identificati tramite richieste di assistenza, segnalazioni dei dipendenti, notifiche dei fornitori o altri fattori che attivano un'indagine.

---

3. Priorità di ripristino

Durante un incidente grave, le priorità di ripristino di ProcessMind sono generalmente:

1. Proteggere l'integrità dei dati dei clienti e prevenire ulteriori danni.
2. Contenere l'incidente e stabilizzare i sistemi interessati.
3. Ripristinare i percorsi di accesso principali alla produzione e i flussi di lavoro critici.
4. Convalidare il comportamento del servizio, l'integrità dei dati e il monitoraggio prima di dichiarare completato il ripristino.
5. Comunicare gli aggiornamenti sullo stato, l'impatto sui clienti e le azioni successive.

La sequenza esatta può variare a seconda della natura dell'incidente, incluso il fatto che incida sull'integrità dei dati, sull'accesso dei clienti, sull'elaborazione asincrona o sull'infrastruttura di supporto.

---

4. Procedure di ripristino di emergenza

4.1 Dichiarazione e coordinamento dell'incidente. Le interruzioni sostanziali del servizio e gli incidenti di sicurezza sono sottoposti a triage tramite procedure di risposta agli incidenti. ProcessMind designa un responsabile dell'incidente, limita la partecipazione alla risposta al personale autorizzato, valuta la gravità e l'ambito, coordina i responsabili tecnici e monitora le azioni di ripristino fino alla risoluzione o alla declassificazione dell'incidente.

4.2 Contenimento. ProcessMind compie sforzi commercialmente ragionevoli per arrestare o ridurre l'impatto in corso prima di avviare un ripristino più ampio. A seconda della modalità di guasto, le azioni di contenimento possono includere il rollback di modifiche recenti, la

disabilitazione dei percorsi interessati, l'isolamento dei componenti malfunzionanti, la sospensione dell'elaborazione in background durante l'esecuzione dei controlli di integrità, la revoca o rotazione delle credenziali o il blocco delle attività abusive.

4.3 Eradicazione. Dopo aver stabilizzato l'impatto immediato, ProcessMind opera per rimuovere la causa alla radice o la condizione che vi contribuisce. Ciò può includere l'applicazione di correzioni al codice o alla configurazione, la rimozione di artefatti dannosi, la rotazione dei segreti, il ripristino di una configurazione attendibile o la chiusura dei percorsi di accesso esposti.

4.4 Ripristino del database. Aurora PostgreSQL esegue backup automatizzati continui con una finestra di conservazione di sette (7) giorni e supporta il ripristino point-in-time. Qualora un guasto a livello di database, un evento di corruzione o una modifica distruttiva accidentale richieda un ripristino, ProcessMind può ripristinare dal backup idoneo più recente o a un punto selezionato nel tempo, convalidare l'ambiente ripristinato e reindirizzare il traffico dell'applicazione al percorso del database ripristinato.

4.5 Ripristino di oggetti e artefatti. I caricamenti di file dei clienti e gli artefatti operativi sono memorizzati in Amazon S3. Il versioning è abilitato nel bucket dei caricamenti e nei bucket delle risorse per supportare il ripristino in caso di eliminazione o sovrascrittura accidentale. I bucket di distribuzione del sito web e del frontend sono trattati come artefatti riproducibili e possono essere ricostruiti dal codice sorgente anziché essere ripristinati come backup.

4.6 Ripristino dei carichi di lavoro asincroni. I percorsi di elaborazione asincrona utilizzano dead-letter queue per conservare gli eventi non riusciti ai fini dell'indagine. Il ripristino può includere il nuovo tentativo dei messaggi non riusciti, la riesecuzione della logica di elaborazione o la riproduzione del lavoro qualora il flusso di lavoro sottostante supporti una rielaborazione sicura.

4.7 Ricostruzione dell'applicazione e dell'infrastruttura. L'infrastruttura è gestita tramite definizioni infrastructure-as-code sottoposte a controllo del codice sorgente. Qualora sia necessario ricreare l'infrastruttura dell'applicazione o gli asset statici, ProcessMind può ricostruire e ridistribuire i componenti interessati a partire dalle definizioni sottoposte a controllo della versione e dagli artefatti di build.

4.8 Convalida prima del ritorno al servizio. Prima della chiusura di un incidente, ProcessMind convalida lo stato del servizio utilizzando il monitoraggio disponibile, i log, i controlli sintetici e verifiche funzionali mirate, e ripristina le funzionalità interessate utilizzando procedure convalidate di distribuzione, ripristino e infrastruttura. Può essere effettuata un'ulteriore revisione quando l'incidente ha comportato il ripristino dei dati o un rischio per l'integrità dei dati.

---

5. Misure di continuità operativa

5.1 Continuità operativa. ProcessMind mantiene procedure operative documentate affinché la gestione degli incidenti, la presa in carico delle richieste di assistenza dei clienti, la risposta tecnica e il processo decisionale possano proseguire durante eventi di interruzione.

5.2 Comunicazioni. Per gli incidenti sostanziali in produzione, ProcessMind compie sforzi commercialmente ragionevoli per fornire aggiornamenti tramite i canali di assistenza clienti e, ove opportuno, tramite la pagina pubblica sullo stato del servizio all'indirizzo processmind.com/status.

5.3 Gestione controllata delle modifiche. Per ridurre le interruzioni evitabili e migliorare la continuità nel tempo, viene utilizzato un ciclo di vita dello sviluppo software con difesa in profondità, comprendente più livelli indipendenti di convalida automatizzata, distribuzioni controllate, monitoraggio centralizzato e revisione post-incidente.

5.4 Sicurezza durante il ripristino. Le azioni di ripristino sono eseguite nel rispetto degli stessi principi generali di sicurezza applicabili durante le

normali operazioni, incluso l'accesso con privilegi minimi, la registrazione delle attività operative ove disponibile e l'accesso controllato ai sistemi e ai dati di produzione.

---

6. Sintesi del backup e della protezione dei dati

6.1 Backup del database. I backup automatizzati di Aurora sono crittografati e conservati per sette (7) giorni, con ripristino point-in-time disponibile entro tale finestra di conservazione.

6.2 Protezioni S3. Amazon S3 offre un'elevata durabilità per gli oggetti archiviati. I bucket contenenti dati dei clienti modificabili si basano sulla durabilità e sul versioning all'interno della regione primaria. ProcessMind attualmente non abilita la replica S3 tra regioni per tali bucket.

6.3 Log e diagnostica. I log, gli allarmi e i dati di telemetria centralizzati supportano l'analisi dei guasti e la convalida del ripristino. Tali meccanismi supportano le operazioni di continuità, ma non sono presentati come un prodotto di backup separato.

---

7. Identificazione e triage degli incidenti

7.1 Valutazione iniziale. Gli eventi segnalati sono sottoposti a triage per determinare se soddisfano la definizione di Incidente di sicurezza, quali sistemi o dati potrebbero essere interessati, la portata e la gravità probabili e se sia necessario un contenimento immediato. La conservazione delle prove è gestita in modo adeguato alla natura dell'incidente e ai sistemi coinvolti.

7.2 Reperibilità e escalation. ProcessMind mantiene una copertura di reperibilità per gli incidenti di produzione, inclusa una copertura 24 ore su 24, 7 giorni su 7 per gli incidenti Critici (come definiti nel Service Level Agreement), affinché gli incidenti possano essere riconosciuti e sottoposti a triage in qualsiasi momento.

7.3 Documentazione. ProcessMind documenta i risultati rilevanti delle indagini, le azioni di risposta e le decisioni di ripristino, affinché la cronologia dell'incidente e le conseguenti azioni correttive possano essere riesaminate dopo l'evento.

---

8. Comunicazioni e notifiche

8.1 Comunicazione interna. ProcessMind coordina i responsabili della risposta, i decisori e i canali di supporto affinché la risposta tecnica e la comunicazione con i clienti rimangano allineate per tutto il ciclo di vita dell'incidente.

8.2 Notifica ai clienti. In caso di un Incidente di sicurezza che richieda una notifica ai sensi del DPA o della legge applicabile, ProcessMind informa i clienti interessati senza indebito ritardo e, ove possibile, entro settantadue (72) ore dal momento in cui viene a conoscenza dell'incidente. Le notifiche generalmente includono la natura e la portata dell'incidente, le categorie di dati interessate, se note, le misure adottate per contenere e porre rimedio all'incidente e le azioni raccomandate ai clienti, ove pertinenti.

8.3 Aggiornamenti continui. Qualora l'incidente rimanga attivo o cambino fatti rilevanti, ProcessMind fornisce aggiornamenti successivi man mano che diventano disponibili ulteriori informazioni verificate. Per interruzioni più ampie del servizio di produzione, ProcessMind può inoltre utilizzare i canali di supporto ai clienti e, ove appropriato, la pagina pubblica sullo stato del servizio all'indirizzo processmind.com/status.

---

9. Test, riesame e manutenzione

ProcessMind riesamina queste procedure almeno annualmente e dopo incidenti rilevanti o modifiche architetturali significative, sottopone periodicamente a esercitazione gli elementi pertinenti dell'approccio di risposta e ripristino (quali il ripristino dei backup, la ricostruzione delle implementazioni, il monitoraggio, gli avvisi e le comunicazioni relative agli

incidenti) e integra gli insegnamenti appresi nelle proprie procedure di sicurezza, affidabilità e continuità.

---

10. Limitazioni e confini contrattuali

Il presente documento è una sintesi di alto livello e non descrive in dettaglio operativo ogni runbook interno, percorso di escalation, metodo investigativo o fase di gestione delle prove. Esso non impegna ProcessMind a predisporre un distinto progetto di failover tra regioni, una conservazione in archiviazione immutabile per tutti i bucket modificabili o garanzie indipendenti relative a RTO/RPO oltre quanto espressamente stabilito nell'accordo o nell'ordine applicabile.

In caso di conflitto tra il presente documento e il Customer Agreement, il Data Processing Addendum, il Service Level Agreement applicabili o una norma imperativa, prevalgono tali fonti.