Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 30



VERSIONE 2.0 · DICEMBRE 2026

Procedura di backup e ripristino (runbook)

Che cosa si copia e che cosa no, con quale frequenza e dove; quale copia usare in ciascuno dei quattro casi di ripristino, con i passi, la verifica dell'integrità, la comunicazione agli studi e la misura dell'RTO. È la versione per i Clienti del runbook operativo di Trailgun.

COPIA GIORNALIERA	SECONDA REGIONE	RPO	RTO
02:00 UTC, 14 giorni	Irlanda, cifrata	24 ore	8 ore

PROCEDURA 30 · PROC-30

Backup e ripristino

Tutti i dati della piattaforma stanno su un disco cifrato, copiato ogni giorno in due regioni dell'Unione e prima di ogni rilascio. Questa procedura dice come si torna a una copia, e come si verifica di esserci tornati bene.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-30	Responsabile della sicurezza (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale, dopo ogni prova e ogni ripristino reale	chi amministra la piattaforma; ICT risk e BCM dei Clienti; audit

DOCUMENTI COLLEGATI

documento 11, Continuità operativa, ripristino e incidenti; documento 31, Prova di disaster recovery; documento 25, Risposta agli incidenti; documento 20, Gestione dei cambiamenti; politica P09; documento 12, Percorso di certificazione e piattaforma

1 Scopo e ambito

1.1 La procedura vale per l'ambiente di production; development e staging si ripristinano con gli stessi passi, senza tempi garantiti. Obiettivi: **RPO di 24 ore**, con lo snapshot giornaliero (nei giorni di rilascio la copia pre-rilascio lo accorcia a pochi minuti); **RTO di 8 ore** di calendario dalla dichiarazione dell'incidente, per il guasto dell'istanza, del disco o della zona con ripristino nella stessa regione.

1.2 Ruoli: il Responsabile della sicurezza decide il caso e la copia, esegue o guida i passi, misura i tempi; il Responsabile del piano (CEO) dichiara l'incidente e decide un ripristino in un'altra regione; la comunicazione agli studi segue il documento 25.

2 Che cosa si copia

Tutto lo stato della piattaforma sta su un solo disco dati EBS cifrato: i due database (dati della piattaforma e conversazioni con gli agenti), le cartelle delle pratiche con originali, testi estratti, indici ed elaborati, i materiali, i lotti, gli arrivi da caselle e API, le fatture, la cache del riconoscimento del testo, i certificati HTTPS. Il disco si copia per intero.

LIVELLO	CHE COSA	QUANDO	CONSERVATA	PROTEGGE DA
Snapshot giornaliero	l'intero disco dati, coerente come dopo un arresto improvviso	ogni giorno alle 02:00 UTC	14 giorni	perdita del disco, corruzione, cancellazioni
Copia in Irlanda	lo stesso snapshot, cifrato, in eu-west-1	ogni giorno	14 giorni	perdita della regione di Francoforte
Snapshot pre-rilascio	l'intero disco, etichettato con il commit	prima di ogni rilascio di production	14 giorni	un rilascio o una migrazione difettosi
Copia del database	il database della piattaforma, copia coerente (`VACUUM INTO`) sullo stesso disco	prima di ogni migrazione	ultime 5	una migrazione difettosa (non la perdita del disco)

3 Che cosa non sta nelle copie del disco

- **Utenti, gruppi e fattori di autenticazione**: stanno nel pool di Amazon Cognito, servizio gestito di AWS a Francoforte, con la protezione dalla cancellazione attiva. In un ripristino nella stessa regione non cambiano.
- **Segreti**: stanno in SSM Parameter Store, cifrati; la fonte è custodita fuori dalla piattaforma (documento 23).
- **Immagini dell'app**: nel registro ECR (ultime 15) e comunque ricostruibili dal codice.
- **Infrastruttura**: descritta come codice e ricostruibile; il disco dati è conservato anche se lo stack viene rimosso.
- **File temporanei** del riconoscimento del testo e della trascrizione (1 giorno) e **log** (CloudWatch, CloudTrail), che hanno i loro periodi.

4 Scegliere il caso

SITUAZIONE	CASO	COPIA DA USARE
Una migrazione o un rilascio hanno danneggiato il database; il disco è integro	1 · copia del database	la copia prima della migrazione

SITUAZIONE	CASO	COPIA DA USARE
Dati cancellati o corrotti; il disco è ancora leggibile	2 · ripristino nel disco in uso	lo snapshot buono più recente, giornaliero o pre-rilascio
Il disco è perso o illeggibile; oppure l'istanza o la zona sono guaste	3 · disco nuovo da snapshot	lo snapshot più recente
La regione di Francoforte non è disponibile	4 · copia in Irlanda	la copia più recente in eu-west-1

5 Prima di ogni caso

1. **Dichiarare** l'incidente e annotare l'ora: da lì decorre l'RTO. Notifica agli studi entro 2 ore (documento 25).
2. **Fermare l'app**, perché le scritture non si perdano o non si mescolino; le lavorazioni in corso si interrompono e si riavviano poi senza costi, quelle in coda ripartono da sole.
3. **Fotografare il disco attuale** prima di toccarlo, perché il ripristino stesso si possa annullare e le evidenze restino.

6 Caso 1 · Migrazione difettosa: la copia del database

1. Con l'app ferma, mettere da parte il database danneggiato con un nome che ne indica l'ora, e sostituirlo con la copia fatta prima della migrazione.
2. Controllare l'integrità del database ripristinato (`PRAGMA integrity_check`: deve dare «ok»).
3. Ripubblicare l'immagine precedente, perché la migrazione non si riapplichi (documento 20, ritorno alla versione precedente), e riavviare.
4. I file scritti dopo la copia restano sul disco ma le loro righe mancano: elencarli dalle cartelle delle pratiche e dire agli studi che cosa ricaricare o rilavorare.

7 Caso 2 · Ripristino nel disco in uso (preferito)

1. Scegliere lo snapshot: il giornaliero più recente anteriore al danno, oppure uno pre-rilascio. Annotarne l'ora: la distanza dal danno è l'RPO effettivo.
2. Creare dallo snapshot un volume temporaneo, cifrato, nella zona dell'istanza, senza l'etichetta che lo farebbe copiare dal ciclo di vita degli snapshot, e collegarlo all'istanza.
3. Montarlo in sola lettura senza riapplicare il giornale del file system, controllare l'integrità dei database su una copia, poi riportare il contenuto nel disco in uso, così com'era nello snapshot.
4. Smontare, scollegare e cancellare il volume temporaneo. Il disco in uso, la sua identità, le copie programmate e la definizione dell'infrastruttura restano validi: non c'è nulla da riallineare.
5. Per un ripristino parziale (una sola pratica, su istruzione scritta del Titolare) si riportano solo la sua cartella e le sue righe.

8 Caso 3 · Disco nuovo da snapshot

1. Creare il volume dallo snapshot come nel caso 2; con l'app ferma, scollegare il vecchio disco senza cancellarlo e collegare il nuovo al suo posto. Se l'istanza è guasta, ricrearla dall'infrastruttura come codice nella stessa zona o in un'altra zona di Francoforte.
2. Spostare sul nuovo disco l'etichetta delle copie giornaliere e toglierla dal vecchio.
3. Riallineare la definizione dell'infrastruttura al nuovo disco prima di qualsiasi altro cambiamento dell'infrastruttura, perché un'applicazione successiva non cerchi il vecchio.
4. Conservare il vecchio disco finché il riesame dell'incidente non lo libera.

9 Caso 4 · Perdita della regione di Francoforte

Le copie cifrate in Irlanda contengono l'intero disco dati. Il Responsabile del piano sceglie fra due strade: attendere il ritorno di Francoforte e riportarvi la copia, oppure ricostruire la piattaforma in Irlanda dall'infrastruttura come codice e dalle immagini ricostruite dal codice, con il disco creato dalla copia più recente e un nuovo pool degli utenti (gli utenti vengono invitati di nuovo e riconfigurano l'app di autenticazione), spostando i record DNS. Il lavoro fatto dopo l'ultima copia in Irlanda si rifà. La procedura regionale scritta e provata, con il suo RTO di 24 ore, è la tappa R03 del Percorso; la prima prova completa la tappa R10 (documento 12).

10 Avvio e verifica, in ogni caso

1. Riavviare l'app; all'avvio applica le migrazioni eventualmente mancanti, dopo la propria copia del database. Attendere che `/api/health` risponda.

2 Verificare: integrità di entrambi i database; nessuna migrazione in sospeso (pagina «Sistema» del backoffice); accesso con un utente di prova; apertura di una pratica recente e dei suoi documenti; confronto di un campione di file con le impronte.

3 Annotare l'ora di fine verifica: è la fine dell'RTO. Annotare la copia usata e la sua ora: è l'RPO effettivo.

4 Ricostruire l'elenco delle pratiche create o modificate dopo l'ora della copia e comunicarlo agli studi, che le ricaricano o le riavviano senza costi.

5 Comunicare il ripristino (documento 25) e scrivere nel registro dell'incidente che cosa si è ripristinato, da quale copia, i dati persi e i tempi.

11 Evidenze e riferimenti

11.1 Evidenze: politiche del ciclo di vita degli snapshot e copie in Irlanda; elenco degli snapshot con data, etichetta e regione; registro degli incidenti con RTO e RPO effettivi; verbali delle prove (documento 31).

11.2 Riferimenti: DORA, art. 12 (backup, ripristino e recupero, compreso il ripristino su sistemi separati) e art. 11; per gli intermediari 106 l'art. 16, par. 1, lett. f), DORA e gli artt. 39-40 del Reg. del. (UE) 2024/1774; GDPR, art. 32, par. 1, lett. c); ISO/IEC 27001:2022, controlli 8.13 (backup delle informazioni) e 5.30 (prontezza ICT per la continuità).

Trailgun

On target.

In a flash.

Dai documenti al lavoro finito: agenti AI per pratiche legali e finanziarie.

SICUREZZA E INCIDENTI, 24/7
security@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

PRIVACY E DPO
privacy@trailgun.ai

Procedura 30 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua la politica P09 (backup e ripristino) e il piano di continuità (documento 11). Le prove sono nel documento 31. Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.