Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 31

VERSIONE 2.0 · DICEMBRE 2026

Programma di prova di disaster recovery

Che cosa Trailgun prova, quando, con quali criteri di successo e come lo documenta: la prova automatica di ripristino a ogni verifica del codice, la prova trimestrale sullo snapshot reale in un ambiente isolato, l'esercitazione annuale del piano e la partecipazione ai test dei Clienti.

A OGNI VERIFICA DEL CODICE
prova automatica

OGNI TRIMESTRE
ripristino dello snapshot reale

OGNI ANNO
esercitazione del piano

ESITO
sempre ai clienti DORA

PROGRAMMA 31 · PROC-31

Prova di disaster recovery

Le copie si provano ripristinandole. Ogni prova ha obiettivi scritti prima, un verbale scritto dopo e un esito che il Cliente può leggere.

CODICE	TITOLARE	APPROVATO DA	VERSIONE
PROC-31	Responsabile della sicurezza (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale, con la revisione del piano di continuità	ICT risk, BCM e audit dei Clienti; chi amministra la piattaforma

DOCUMENTI COLLEGATI

documento 11, Continuità operativa, ripristino e incidenti; documento 30, Backup e ripristino; documento 25, Risposta agli incidenti; documento 20, Gestione dei cambiamenti; documento 12, Percorso di certificazione e piattaforma

1 Scopo e ambito

Il programma dimostra che le copie della piattaforma si ripristinano, che i dati ripristinati sono integri e che l'RTO di 8 ore e l'RPO di 24 ore sono rispettati; e che le persone sanno che cosa fare. Copre l'ambiente di production; le prove non toccano mai l'istanza, il disco o le copie di production.

2 Il calendario

PROVA	QUANDO	CHE COSA DIMOSTRA	VERBALE
Prova automatica di ripristino	a ogni verifica del codice: ogni pull request verso un branch di ambiente e ogni rilascio	che le due forme di copia (copia coerente del database e copia grezza del disco, come uno snapshot preso a server acceso) si ripristinano senza differenze	generato dall'integrazione continua e conservato come artefatto
Prova di ripristino sullo snapshot reale	ogni trimestre e dopo ogni cambiamento dell'infrastruttura	che l'ultimo snapshot di production si ripristina, che i database sono integri, quanto valgono l'RPO e l'RTO reali	scritto dallo strumento di prova, firmato e conservato nel repository
Esercitazione a tavolino	ogni anno, con la revisione del piano	ruoli, decisioni, comunicazioni e tempi di notifica, su uno o più scenari S1-S8 del documento 11; raggiungibilità di referenti dei Clienti, sostituti e fornitori	rapporto di esercitazione (tabella 7)
Simulazione di notifica	ogni anno, nell'esercitazione	una notifica completa a un Cliente DORA con i modelli del documento 51, nei tempi del documento 25	nel rapporto di esercitazione

Le prove che arrivano con le prossime tappe stanno nel Percorso (documento 12): la prova completa di ripristino regionale in Irlanda (tappe R03 e R10), il penetration test indipendente (R06) e le prove della nuova piattaforma su più zone (R12).

3 La prova automatica, a ogni verifica

3.1 Il job di prova dell'integrazione continua costruisce un database con lo schema reale e tutte le migrazioni, vi scrive righe e file, lo copia come fa production (copia coerente `VACUUM INTO`, e copia grezza della cartella dei dati presa con una transazione di scrittura aperta, come uno snapshot), ripristina ogni copia in una cartella nuova e verifica: integrità del database, stesso schema, stesse righe in ogni tabella, i file byte per byte con le impronte SHA-256, e che applicare di nuovo le migrazioni alla copia ripristinata non cambi nulla. Misura il tempo di ripristino di ciascuna forma.

3.2 Una differenza fa fallire la verifica, e senza verifica superata nulla arriva su una macchina (documento 20). Lo strumento ha anche una modalità che danneggia apposta le copie ripristinate: la prova deve fallire, e si usa per controllare che la prova stessa funzioni.

4 La prova trimestrale sullo snapshot reale

1 Lo strumento di prova legge, in sola lettura, l'istanza e il disco di production, per tenerli fuori portata, e sceglie lo snapshot giornaliero più recente completato: la sua età è l'RPO dimostrato.

2 Avvia un'istanza temporanea in un gruppo di sicurezza senza alcuna regola in ingresso, raggiungibile solo con SSM, e crea in parallelo un volume dallo snapshot nella stessa zona.

3 Collega e monta il volume come in un ripristino vero, poi esegue sui database il controllo d'integrità, legge la versione dello schema e i conteggi delle righe per tabella, e controlla che gli archivi a cui il database rimanda esistano sul disco. Dall'istanza escono solo conteggi e orari, mai contenuti.

4 In ogni caso, anche in errore, termina l'istanza, cancella il volume e il gruppo di sicurezza, ciascuno solo dopo averne verificato l'etichetta di questa prova; rifiuta di toccare qualsiasi risorsa di production. Il volume ripristinato non porta mai l'etichetta delle copie programmate.

5 Scrive il verbale con snapshot, RPO, RTO, esiti dei controlli e della pulizia; esce con successo solo se tutti i controlli e la pulizia sono riusciti. Il Responsabile della sicurezza lo firma e lo conserva.

5 Criteri di successo

- Controllo d'integrità «ok» su tutti i database ripristinati; versione dello schema attesa; conteggi coerenti con production all'ora dello snapshot.
- Gli archivi a cui il database rimanda sono presenti sul disco ripristinato.
- Età dello snapshot entro l'RPO di 24 ore; tempo dalla dichiarazione simulata alla fine delle verifiche entro l'RTO di 8 ore.
- Pulizia completa delle risorse di prova, verificata, e nessuna azione su risorse di production.

Una prova che non raggiunge un criterio non è fallita se ne esce un'azione correttiva con titolare e data, scritta nel verbale e nel registro dei rischi (documento 41); la prova si ripete dopo la correzione.

6 La prima prova sullo snapshot reale

La prima prova trimestrale sullo snapshot di production si è svolta il [data], sullo snapshot del [data e ora]: RPO dimostrato [hh:mm], RTO misurato [hh:mm], integrità dei database [ok], pulizia [completa], esito [superata]. Il verbale è disponibile ai Clienti che lo chiedono.

7 · RAPPORTO DI ESERCITAZIONE A TAVOLINO	CHE COSA SCRIVERE	CONTENUTO
Data, durata, partecipanti	ruoli coperti; Clienti presenti	
Scenario e sviluppi	S1–S8; informazioni introdotte durante l'esercitazione	
Decisioni prese e tempi	attivazione, classificazione, notifica: ore simulate	
Comunicazioni prodotte	notifica iniziale e aggiornamenti redatti con i modelli	
Contatti verificati	raggiunti, non raggiunti, aggiornati	
Lacune emerse	contatti, accessi, procedure, decisioni senza un titolare	
Azioni	con titolare e data	
Firma	Responsabile del piano	

8 Esiti ai Clienti e test dei Clienti

8.1 L'esito di ogni prova di ripristino si comunica al Cliente che lo chiede e sempre ai Clienti DORA: data, snapshot, RPO e RTO misurati, esito, azioni correttive. Il Cliente DORA può partecipare all'esercitazione annuale.

8.2 Trailgun partecipa, alle condizioni concordate per non mettere a rischio gli altri Clienti, ai test di continuità e ai test guidati dalla minaccia dei Clienti che vi sono tenuti (art. 26 DORA), anche in forma congiunta. Gli intermediari 106 non sono tenuti al TLPT (art. 6 D.Lgs. 23/2025).

9 Evidenze e riferimenti

9.1 Evidenze: verbali della prova automatica (artefatti dell'integrazione continua); verbali firmati delle prove trimestrali; rapporti delle esercitazioni; azioni correttive nel registro dei rischi.

9.2 Riferimenti: DORA, art. 11, par. 4 e 6, art. 12, par. 3 e 6, artt. 24-26 e art. 30, par. 3, lett. c) e d); per gli intermediari 106 l'art. 16, par. 1, lett. f) e g), DORA; Reg. del. (UE) 2024/1774, art. 25 e artt. 39-40; GDPR, art. 32, par. 1, lett. d); ISO/IEC 27001:2022, controlli 5.29, 5.30 e 8.13.

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

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