Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P09



VERSIONE 2.0 · DICEMBRE 2026

Politica di backup e ripristino

Quali copie esistono, dove, per quanto tempo, come si proteggono e come si prova che funzionano: a ogni verifica della CI e ogni trimestre sullo snapshot reale, con l'RTO misurato e il verbale.

CODICE	TITOLARE	REVISIONE	STATO
P09 · POL-09	Responsabile della sicurezza	Annuale · dopo ogni prova	al 01/12/2026

POLITICA P09 · POL-09

Politica di backup e ripristino

Quali copie esistono, dove, per quanto tempo, come si proteggono e come si prova che funzionano. I passi del ripristino sono nella procedura 30.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P09 (POL-09)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale e dopo ogni prova di ripristino	personale tecnico; uffici ICT risk e continuità operativa dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P04, P12; documento 11 (Continuità operativa, ripristino e incidenti); procedura 30 (Backup e ripristino); procedura 31 (Programma di prova di disaster recovery); documento 12 (Percorso di certificazione e piattaforma)

AMBITO

Il disco dati di ogni ambiente (database, documenti, elaborati, indici, materiali, fatture) e la configurazione necessaria a ricostruire il servizio (infrastruttura come codice, immagini, segreti).

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.13, 8.14, 5.30	DORA artt. 11, 12; GDPR art. 32(1)(c)

1 Scopo e ruoli

Le copie servono solo se si ripristinano. Il Responsabile della sicurezza definisce le copie, ne verifica l'esito, guida i ripristini e le prove e firma i verbali; il piano di continuità (documento 11) decide quando ripristinare.

2 Le copie

Tutto lo stato della piattaforma sta su un disco dati cifrato: database, cartelle delle pratiche, materiali, archivi, testi estratti, certificati. Le copie sono queste.

COPIA	FREQUENZA	CONSERVAZIONE	LUOGO
Snapshot giornaliero dell'intero disco	ogni 24 ore alle 02:00 UTC	14 in production (7 staging, 3 development)	Francoforte, cifrato
Copia in Irlanda	di ogni snapshot giornaliero di production	14 giorni	eu-west-1, cifrata
Snapshot prima del rilascio	a ogni rilascio di production, con il commit come etichetta	14 giorni	Francoforte, cifrato
Copia del database prima delle migrazioni	a ogni migrazione	ultime 5	stesso disco: serve a un ritorno rapido, non è una copia di sicurezza

3 Regole

3.1 **Obiettivi.** RPO di 24 ore; RTO di 8 ore per un guasto dell'istanza, del disco o della zona, con ripristino nella stessa regione. Lo snapshot ogni 4 ore (tappa R01), il ripristino regionale in Irlanda con il suo RTO (tappa R03) e gli obiettivi della nuova piattaforma (tappa R14) sono nel Percorso.

3.2 **Cifratura e rotazione.** Ogni copia è cifrata e si conserva 14 giorni; dopo la cancellazione di dati da parte del Titolare, le copie che li contengono escono per rotazione entro 14 giorni.

3.3 **Separazione.** Le copie stanno in due regioni dell'UE. Il volume dei dati si conserva anche se si rimuove lo stack. Le copie protette dalla cancellazione per 7 giorni sono la tappa R11.

3.4 **Ripristino su risorse nuove.** Si ripristina su un volume nuovo, mai sovrascrivendo l'originale, e lo si verifica prima di metterlo in servizio: controllo d'integrità dei database, versione dello schema, conteggio delle righe per tabella, presenza sul disco degli archivi a cui il database rimanda.

3.5 **Ciò che sta fuori dal disco.** Il pool degli utenti, i segreti e le immagini non sono nel disco dati: l'infrastruttura come codice e la procedura 30 dicono come ricostruirli; in un ripristino del pool gli utenti ricevono un nuovo invito e registrano di nuovo l'app di autenticazione.

3.6 **Primo ripiego dell'avvocato.** Il Cliente scarica in ogni momento i propri elaborati; per l'avvocato che deve depositare, l'elaborato già scaricato è il primo ripiego durante un'interruzione.

4 Le prove

1 **A ogni verifica della CI.** Una prova automatica crea una base di dati con lo schema reale, ne fa le copie nei due modi in cui la piattaforma le fa (copia coerente del database e copia dell'intero disco durante una scrittura), le ripristina e verifica integrità, schema, righe e file byte per byte. Se la prova fallisce, il rilascio non parte.

2 **Ogni trimestre, sullo snapshot reale.** L'ultimo snapshot di production si ripristina su un'istanza temporanea isolata, senza porte aperte; si verificano i database e gli archivi, si misurano RPO e RTO; dall'istanza escono solo conteggi e orari, mai contenuti; istanza e volume si cancellano a fine prova.

3 **Verbale.** Ogni prova trimestrale produce un verbale con snapshot usato, RPO e RTO misurati, esito dei controlli e della pulizia; l'esito si comunica al Cliente che lo chiede e sempre ai Clienti DORA.

4 **Prova regionale.** La prova completa di ripristino in Irlanda, annuale, è la tappa R10 del Percorso (procedura 31).

5 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Snapshot e copia in Irlanda	IN ESSERE 14 snapshot giornalieri e 14 giorni di copie	infrastruttura come codice; elenco degli snapshot
Scadenza delle copie pre-rilascio	IN ESSERE 14 giorni	script di rilascio; elenco degli snapshot
Prova automatica	IN ESSERE a ogni verifica della CI, con il risultato conservato	a ogni pull request e rilascio
Prova trimestrale	IN ESSERE prima prova sullo snapshot di production del [data], RTO misurato [...]	verbale, ogni trimestre

6 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione sospende la prova trimestrale per più di un trimestre. Riferimenti: DORA artt. 11 e 12 (ripristino su sistemi separati, par. 3; RTO e RPO coerenti con i livelli di servizio, par. 6); GDPR art. 32, par. 1, lett. c); ISO/IEC 27001:2022 controlli 5.30, 8.13, 8.14.