Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P05

VERSIONE 2.0 · DICEMBRE 2026

Politica delle operazioni e dei cambiamenti

Come Trailgun gestisce ambienti, configurazioni, capacità e rilasci, e come ogni cambiamento arriva in production con la verifica superata, una copia del disco e nessuna sorpresa per i Clienti.

CODICE	TITOLARE	REVISIONE	STATO
P05 · POL-05	Responsabile della sicurezza	Annuale	al 01/12/2026

POLITICA P05 · POL-05

Politica di sicurezza delle operazioni e gestione dei cambiamenti

Ambienti, configurazione, capacità e rilasci: come ogni cambiamento arriva in production senza sorprese per i Clienti.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P05 (POL-05)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	personale tecnico; uffici ICT risk e audit dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P06, P07, P09; procedura 20 (Gestione dei cambiamenti); registro dei cambiamenti (45); documento 11 (Continuità operativa, ripristino e incidenti)

AMBITO

Codice dell'app, immagini dei container, infrastruttura (AWS CDK), configurazione e segreti, prompt del registro, modelli assegnati agli agenti, fornitori collegati.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.37, 8.6, 8.7, 8.9, 8.19, 8.31, 8.32	DORA art. 9(4)(e); Reg. del. (UE) 2024/1774

1 Scopo e ruoli

Un servizio stabile nasce da ambienti separati, da una configurazione descritta come codice e da cambiamenti che seguono sempre lo stesso percorso. Il Responsabile della sicurezza approva i cambiamenti dell'infrastruttura e i cambiamenti urgenti, tiene il registro dei cambiamenti (45) e decide le finestre di manutenzione; chi sviluppa apre la pull request e ne risponde.

2 Ambienti

2.1 Tre ambienti online, ciascuno con il proprio stack, la propria macchina, il proprio disco, IP, registro delle immagini, parametri, log, bucket e pool di utenti: development (app.dev.trailgun.ai), staging (app.staging.trailgun.ai), production (app.trailgun.ai).

2.2 Development e staging usano di default servizi esterni di prova (banca dati, posta, notifiche, firma). Lo script di rilascio impone a ciascun ambiente il pool di utenti del suo stack, così una configurazione copiata da production non fa entrare gli utenti veri.

2.3 I dati di production non si copiano negli altri ambienti né sui computer del personale. Prove e dimostrazioni usano dati sintetici.

3 Configurazione e capacità

3.1 L'infrastruttura è descritta come codice (AWS CDK) ed è ricostruibile. L'immagine del sistema operativo dell'istanza riceve gli aggiornamenti di sicurezza ogni mese; l'immagine del proxy Caddy è fissata a una versione e si aggiorna con un cambiamento ordinario; il container dell'app gira con un utente non privilegiato.

3.2 Spazio disco, CPU, memoria, errori 5xx e scadenza dei certificati sono sotto allarme 24/7 (politica P08). Le immagini conservate nel registro sono le ultime 15; le copie del database prima delle migrazioni sono le ultime 5.

4 Tipi di cambiamento

4.1 **Ordinario: rilascio dell'app.** Branch di lavoro, pull request verso development, poi promozione per branch di ambiente: staging, production. I branch di ambiente sono protetti: si aggiornano solo con pull request e con la verifica superata. Una promozione diretta da development a production segue le stesse regole e si annota nel registro.

4.2 **Infrastruttura.** `cdk deploy` solo a mano, con lo stack nominato, approvato dal Responsabile della sicurezza; mai dalla CI.

4.3 **Prompt e modelli.** Il testo dei prompt si cambia solo dal backoffice della piattaforma e non esce mai verso il browser di uno studio; lo studio può solo aggiungere testi propri. Un cambio del modello predefinito di un agente è un cambiamento rilevante (politica P15).

4.4 **Urgente** (sicurezza, ripristino). Si esegue subito, si documenta nel registro entro il giorno lavorativo successivo con motivo e verifica, e si comunica ai Clienti come intervento urgente.

5 Il percorso di un rilascio

1. **Verifica obbligatoria.** Controllo dei tipi del server, del frontend e dell'infrastruttura; test unitari; test end-to-end dell'interfaccia; scansione dei segreti su tutta la storia del repository; prova di ripristino del database. Se uno di questi passi fallisce, il rilascio non parte.
2. **Immagine.** Costruita in CI con il commit come etichetta e analizzata dal registro delle immagini al caricamento.
3. **Production solo dal suo branch.** Il rilascio di production parte solo dal branch `production` e rifiuta un commit che non ha superato la verifica, anche quando è lanciato a mano.
4. **Copia prima del rilascio.** Il disco dati si fotografa (snapshot con il commit come etichetta, conservato 14 giorni).
5. **Nessuna lavorazione interrotta.** Il rilascio si rifiuta se ci sono atti del modulo in lavorazione; forzarlo è un cambiamento urgente da documentare. Le lavorazioni in coda ripartono da sole.
6. **Migrazioni.** All'avvio l'app applica le migrazioni del database: numerate, solo in avanti, mai modificate dopo la pubblicazione e compatibili con l'immagine precedente, così il ritorno all'immagine precedente non richiede di toccare i dati.
7. **Controllo di salute.** Il rilascio verifica `/api/health` prima di dichiararsi concluso; la riga del registro dei cambiamenti riporta esito e snapshot.

6 Finestre e comunicazione

La manutenzione programmata si annuncia con almeno 48 ore di preavviso, si svolge tra le 20:00 e le 07:00 o nel fine settimana, per non più di 8 ore al mese, mai nella finestra lavorativa. I rilasci ordinari durano meno di 2 minuti e avvengono solo senza lavorazioni del modulo in corso; una lavorazione interrotta si riavvia senza costi. I cambi di subfornitori seguono i preavvisi della politica P10.

7 Protezione dal codice malevolo

I file caricati non si eseguono mai: si leggono e si convertono con componenti dedicati (pdf.js, LibreOffice, Chromium) nel container dell'app, che gira senza privilegi. Gli archivi hanno limiti sul numero di voci (5.000) e sulla dimensione contro gli zip bomb. Il penetration test indipendente (Percorso, tappa R06) verifica anche questi percorsi; il filtro applicativo (WAF) arriva con la nuova piattaforma (tappa R12).

8 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Ambienti separati, infrastruttura come codice	IN ESSERE tre stack, un pool di utenti ciascuno	repository dell'infrastruttura
Branch protetti e verifica obbligatoria	IN ESSERE anche per il rilascio di production lanciato a mano	esito della verifica nella pull request
Snapshot prima del rilascio	IN ESSERE con il commit come etichetta, 14 giorni	a ogni rilascio di production
Registro dei cambiamenti	IN ESSERE pull request, tipo, verifica, approvazione, migrazione, snapshot, esito	foglio 45, a ogni rilascio
Aggiornamenti del sistema e del proxy	IN ESSERE immagine aggiornata ogni mese; Caddy a versione fissata; container non root	registro dei cambiamenti

9 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette un rilascio di production senza verifica superata. Riferimenti: DORA art. 9, par. 4, lett. e); Reg. del. (UE) 2024/1774; ISO/IEC 27001:2022 controlli 5.37, 8.6, 8.7, 8.9, 8.19, 8.31, 8.32.