Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 25



VERSIONE 2.0 · DICEMBRE 2026

Procedura di risposta agli incidenti (runbook)

Il runbook che Trailgun segue per ogni incidente che tocca o può toccare il servizio o i dati dei Clienti: rilevazione, classificazione a tre livelli sui criteri del Regolamento delegato (UE) 2024/1772, contenimento, notifica, ripristino, riesame. Costruito perché il Cliente soggetto a DORA possa classificare e segnalare nei suoi tempi.

NOTIFICA INIZIALE	AGGIORNAMENTI	RELAZIONE INTERMEDIA	RELAZIONE FINALE
2 ore	almeno ogni 24 ore	48 ore	20 giorni

PROCEDURA 25 · PROC-25

Risposta agli incidenti TIC

Che cosa fa Trailgun, in quale ordine e in quanto tempo, da quando osserva un evento a quando il Cliente riceve la relazione finale.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-25	Responsabile della sicurezza (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale e dopo ogni incidente grave	chi gestisce il servizio; ICT risk, SOC e DPO dei Clienti

DOCUMENTI COLLEGATI

documento 11, Continuità operativa, ripristino e incidenti; documento 26, Violazioni dei dati personali; documento 30, Backup e ripristino; documento 23, Chiavi e segreti; documento 51, Modelli di notifica degli incidenti; documento 18, Allegato DORA al contratto; documento 55, Accordo sul livello di servizio

1 Scopo, ambito e definizioni

1.1 La procedura vale per ogni incidente che incide o può incidere sulla piattaforma di production, sui dati dei Clienti o sui processi che servono a erogarla, compresi gli incidenti che nascono presso un fornitore.

1.2 **Evento**: qualsiasi fatto osservato che può riguardare la sicurezza o la disponibilità (un allarme, un errore, una segnalazione). **Incidente TIC**: un evento, o una serie di eventi collegati, non pianificato, che compromette o può compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o del servizio (art. 3 DORA). **Minaccia informatica significativa**: una minaccia che può colpire il servizio o i Clienti, anche prima che si traduca in un incidente. **Violazione dei dati personali**: art. 4, punto 12, GDPR; segue anche il documento 26.

1.3 La qualifica di «incidente grave» ai sensi dell'art. 19 DORA la decide il Cliente sui propri criteri. La classificazione di Trailgun gli dà in tempo i dati per farlo, ed è volutamente più prudente: basta un criterio per il livello più alto.

2 Ruoli e reperibilità

RUOLO	COMPITI	TITOLARE E SOSTITUTO
Gestore dell'incidente	apre la voce nel registro, classifica, guida contenimento e ripristino, annota ogni passo con l'ora	Responsabile della sicurezza; sostituto [nome]
Comunicazione	notifiche ai Clienti nei tempi del paragrafo 6, aggiornamenti, messaggi agli studi	Responsabile della sicurezza; sostituto [nome]
Protezione dei dati	valuta se c'è violazione dei dati personali e guida il documento 26	DPO [DPO esterno: nome o società]
Responsabile del piano	attiva il piano di continuità (documento 11), decide il ripristino, informa l'organo amministrativo degli incidenti gravi	CEO
Supporto esterno	assistenza AWS, analisi forense, consulenza legale	[contratti e contatti]

La reperibilità per le priorità 1 è attiva 24/7 al numero [+39 …]. La casella **security@trailgun.ai** è presidiata 24/7 per le priorità 1 e risponde in automatico con il numero di reperibilità. I contatti dei referenti dei Clienti, dei sostituti e dei fornitori si tengono anche fuori dalla piattaforma, in copia cifrata accessibile al sostituto.

3 Da dove arrivano gli eventi

- Sonda esterna ogni minuto su `/api/health` e sull'avvio di una lavorazione; allarmi 24/7 su salute, disco, CPU, memoria, errori 5xx e scadenza dei certificati.
- GuardDuty e CloudTrail (tutte le regioni, convalida dell'integrità); sessioni SSM registrate.
- Log di accesso HTTP e log applicativi (90 giorni, senza corpo delle richieste, token né testo dei documenti); registro delle attività degli studi; registro degli accessi ai fascicoli penali.
- Segnalazioni dei Clienti (in app, email, telefono di reperibilità), dei fornitori, dei ricercatori (documento 24) e del personale.

4 Le fasi, passo per passo

1 **Registrare.** Ogni evento rilevante si annota nel registro degli incidenti con ora, fonte e descrizione; un incidente riceve un codice INC-*aaaa-nnn*, usato in tutte le comunicazioni. Il registro raccoglie tutti gli incidenti e le minacce significative (art. 17, par. 2, DORA).

2 **Classificare** entro la prima ora con la tabella 5 e la matrice, e di nuovo a ogni informazione nuova. Annotare l'ora in cui l'evento è qualificato come incidente: da lì decorrono le 2 ore della notifica.

3 **Preservare le evidenze** prima di cambiare qualsiasi cosa: snapshot del disco nello stato in cui si trova, esportazione dei log disponibili, schermate degli allarmi.

4 **Contenere.** Fermare il danno: revoca delle credenziali (paragrafo 8), isolamento dell'istanza, sospensione di una funzione o di un fornitore, manutenzione urgente. Se il servizio è o può restare indisponibile oltre 2 ore, o i dati sono a rischio, attivare il piano di continuità (documento 11).

5 **Notificare** ai Clienti interessati entro 2 ore, anche con informazioni parziali (paragrafo 6), con il modello di notifica iniziale (documento 51). Se ci sono dati personali coinvolti, avviare in parallelo il documento 26.

6 **Eliminare la causa e ripristinare** con le procedure del documento 30 (backup e ripristino), del documento 20 (ritorno alla versione precedente) o con la ricostruzione pulita (paragrafo 8).

7 **Chiudere** quando il servizio è ripristinato e verificato e la causa è rimossa o mitigata; comunicarlo ai Clienti.

8 **Riesaminare** (art. 13, par. 2, DORA): cause, tempi, che cosa ha funzionato e che cosa no, azioni con titolare e data, aggiornamento del registro dei rischi (documento 41) e, se serve, del piano e delle procedure. L'esito va nella relazione finale.

5 Classificazione

Tre livelli, sui criteri del Reg. del. (UE) 2024/1772: servizi critici colpiti, perdite di dati, durata e tempo di inattività, clienti colpiti, diffusione geografica, impatto economico e reputazionale, ricorrenza. Vale il livello più alto fra quelli che un criterio fa scattare.

CRITERIO	GRAVE	SIGNIFICATIVO	MINORE
Perdite di dati	accesso non autorizzato riuscito, o sospetto fondato, ai dati di un Cliente; perdita di dati oltre l'RPO; qualsiasi dato di un fascicolo penale	perdita entro l'RPO, recuperata; errore d'integrità circoscritto e corretto	nessun dato dei Clienti coinvolto
Inattività e durata	servizio o funzione principale indisponibile oltre 2 ore, o incidente aperto oltre 24 ore	indisponibilità fino a 2 ore; funzione degradata oltre 2 ore	nessuna indisponibilità percepita dai Clienti
Servizi colpiti	accesso, consultazione o lavorazioni	una funzione accessoria (comunicazioni, firma, ricerca fonti)	ambienti non di produzione, strumenti interni
Clienti colpiti	più Clienti, o un Cliente DORA per una funzione essenziale o importante	un Cliente	un singolo utente, con ripiego
Diffusione geografica	Trailgun indica gli Stati membri dei Clienti colpiti; il criterio lo applica il Cliente (soglia: due o più Stati membri)		
Impatto economico e reputazionale	attenzione dei media, reclami di più Clienti, coinvolgimento di un'autorità	reclamo di un Cliente	–
Ricorrenza	due incidenti con la stessa causa apparente in sei mesi si considerano insieme e il livello si rivaluta sul totale		
Priorità di assistenza	1 · Bloccante	2 · Grave	3 · Ordinaria

Il criterio del Cliente. Per il Reg. del. (UE) 2024/1772, art. 8, un incidente che colpisce servizi critici è grave se c'è un accesso malevolo non autorizzato riuscito che può portare a perdite di dati, oppure se si superano due o più delle altre soglie dell'art. 9: clienti colpiti oltre il 10 % o oltre 100.000; durata oltre 24 ore o inattività oltre 2 ore per i servizi che supportano funzioni essenziali o importanti; due o più Stati membri; impatto economico oltre 100.000 euro. La tabella di Trailgun scatta prima, perché il Cliente abbia i dati in tempo.

Matrice per il triage

Impatto sui dati per righe, impatto sul servizio per colonne. Se la matrice e la tabella danno livelli diversi, vale il più alto.

DATI ↓ · SERVIZIO →	NESSUN EFFETTO	FUNZIONE DEGRADATA	INDISPONIBILE FINO A 2 ORE	INDISPONIBILE OLTRE 2 ORE
ACCESSO NON AUTORIZZATO, DATI PENALI, PERDITA OLTRE L'RPO	Grave	Grave	Grave	Grave

DATI ↓ · SERVIZIO →	NESSUN EFFETTO	FUNZIONE DEGRADATA	INDISPONIBILE FINO A 2 ORE	INDISPONIBILE OLTRE 2 ORE
PERDITA ENTRO L'RPO, ERRORE D'INTEGRITÀ CORRETTO	Significativo	Significativo	Significativo	Grave
NESSUN DATO COINVOLTO	Minore	Significativo	Significativo	Grave

6 Tempi di notifica al Cliente

PASSO	TRAILGUN	COME	MODELLO (DOCUMENTO 51)
Notifica iniziale	entro 2 ore dalla conoscenza	email ai referenti del Modulo d'ordine e telefono al referente	notifica iniziale
Aggiornamenti	almeno ogni 24 ore e a ogni cambiamento rilevante; per le priorità 1 ogni 2 ore fino al ripristino	email	aggiornamento
Relazione intermedia	entro 48 ore dalla notifica iniziale	email	relazione intermedia
Relazione finale	entro 20 giorni dalla chiusura, e comunque in tempo per la relazione finale del Cliente entro un mese	email	relazione finale
Minaccia significativa	entro 24 ore	email	minaccia
Violazione dei dati personali	entro 24 ore al Titolare	email al referente sicurezza e al DPO	documento 26

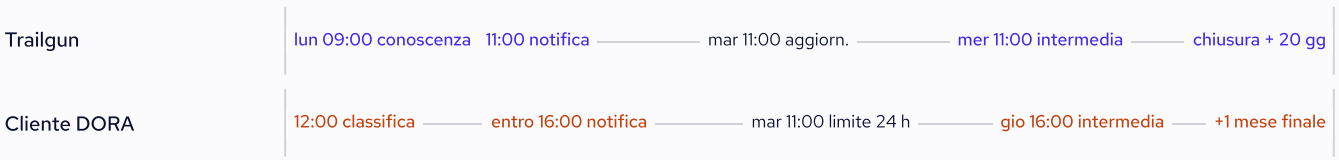
6.1 I tempi sono in ore di calendario, anche nei fine settimana e nei festivi. Un campo che non si conosce ancora si scrive «in verifica» con l'ora prevista: non si omette.

6.2 L'assistenza al Cliente nella gestione di un incidente legato al servizio è senza costi aggiuntivi (art. 30, par. 2, lett. f), DORA). Trailgun non presenta segnalazioni alle autorità per conto del Cliente salvo accordo scritto; anche in quel caso il Cliente ne resta pienamente responsabile (art. 19, par. 5, DORA).

6.3 Gli incidenti minori che non toccano il Cliente si registrano e compaiono nell'estratto del registro che il Cliente può chiedere in ogni momento.

7 I tempi di Trailgun accanto a quelli del Cliente

Trailgun viene a conoscenza di un incidente lunedì alle 09:00 e lo notifica alle 11:00. In alto i termini di Trailgun, in basso quelli del Cliente DORA che lo classifica come grave alle 12:00 (Reg. del. (UE) 2025/301, art. 5).



Il Cliente invia la notifica iniziale entro 4 ore dalla classificazione e comunque entro 24 ore dalla conoscenza; la relazione intermedia entro 72 ore dalla notifica iniziale; la finale entro un mese dall'ultima intermedia. Se il termine cade nel fine settimana o in un festivo, alcune entità possono presentare entro mezzogiorno del giorno lavorativo successivo; l'eccezione non vale per gli enti creditizi (art. 5, par. 4-5). I tempi di Trailgun non dipendono da questa eccezione.

8 Contenimento: credenziali compromesse (RB-05)

1 Disattivare subito le credenziali sospette: sessioni di IAM Identity Center e sessioni SSM aperte, utente Cognito (disattivazione e disconnessione globale), chiavi API dello studio coinvolto (revoca dall'Organizzazione o dal backoffice), account presso i fornitori.

2 Ruotare i segreti coinvolti con il documento 23 e riavviare l'app perché li carichi.

3 Ricostruire dai log (CloudTrail, log di accesso HTTP, registro delle attività, log applicativi) che cosa è stato fatto con le credenziali; valutare la violazione dei dati personali (documento 26).

9 Contenimento: isolamento e ricostruzione pulita (RB-08)

1 Preservare le evidenze: snapshot di tutti i volumi ed esportazione dei log, prima di ogni modifica.

2 Isolare l'istanza (chiusura del traffico in ingresso dal gruppo di sicurezza; arresto se l'attacco è in corso) e applicare il paragrafo 8 a tutte le credenziali.

3 Ricostruire istanza e container dall'infrastruttura come codice e da un'immagine verificata; ripristinare i dati dall'ultima copia anteriore alla compromissione, verificata su un volume isolato (documento 30).

4 Riaprire il servizio solo dopo la verifica del Responsabile della sicurezza; analisi forense con [fornitore] se serve. Nessun pagamento di riscatto.

10 Registro degli incidenti

10.1 Per ogni incidente e minaccia significativa: codice, ora di rilevazione e di conoscenza, classificazione e sue revisioni, Clienti e funzioni colpiti, dati coinvolti, fornitore d'origine, comunicazioni inviate con l'ora, misure, ora di chiusura, RTO e RPO effettivi, causa radice, azioni correttive con titolare e data, collegamento all'eventuale violazione dei dati personali.

10.2 Il registro è tenuto da Trailgun; al Cliente si consegna l'estratto delle voci che lo riguardano, su richiesta e in audit. Vi è registrato l'incidente operativo di disponibilità del 21/10/2026 (riavvio di production non riuscito per il disco di sistema pieno), senza perdita né esposizione di dati, con le sue azioni correttive (pulizia delle immagini locali inutilizzate a ogni rilascio, che restano nel registro ECR, e allarme sullo spazio disco).

11 Riferimenti

DORA, artt. 17-19 e art. 30, par. 2, lett. f); Reg. del. (UE) 2024/1772 (classificazione, artt. 8 e 9); Reg. del. (UE) 2025/301 (contenuti e termini, art. 5); Reg. es. (UE) 2025/302 (moduli di segnalazione, con il campo sull'origine presso un fornitore terzo); art. 16, par. 1, DORA e art. 6 D.Lgs. 23/2025 per gli intermediari 106; GDPR, artt. 33 e 34; ISO/IEC 27001:2022, controlli 5.24-5.28 e 6.8.

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 25 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Il piano di continuità è il documento 11; i modelli di notifica sono il documento 51; le violazioni dei dati personali seguono anche il documento 26. Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.