SECURITY & COMPLIANCE

Sicurezza del ciclo di vita del software, vulnerabilità e aggiornamenti

Ciclo di sviluppo, gestione dipendenze e correzione vulnerabilità.

Prodotto	ClaimEvidence
Codice	CLE-PUB-20-IT
Edizione documentale	Edizione del 30 agosto 2026
Efficacia / riesame	2026-08-30 / 2027-02-28
Titolare del documento	Nil Tech Europe S.r.l. · Compliance & Security
Classificazione	Pubblico

Preambolo, natura ed efficacia del documento

Nil Tech Europe S.r.l., con sede legale in Via Calmaggiore 5, 31100 Treviso (TV), Italia, P. IVA IT 05614380268 (di seguito «Niltech»), adotta il presente documento al fine di descrivere come requisiti, codice, dipendenze, test, distribuzione, vulnerabilità e aggiornamenti sono governati lungo il ciclo di sviluppo.

Il documento è un atto societario di trasparenza e accountability. Non costituisce certificazione di terza parte, parere legale destinato a soggetti diversi dalla società, garanzia assoluta di sicurezza o dichiarazione generalizzata di conformità; gli impegni contrattuali derivano esclusivamente dagli accordi applicabili.

Il documento disciplina la sicurezza dell'intero ciclo di vita del software, inclusi requisiti, progettazione, implementazione, verifica, distribuzione, manutenzione e gestione delle vulnerabilità, in coerenza con i principi di protezione fin dalla progettazione e, ove applicabile, con il Cyber Resilience Act.

Ambito soggettivo e oggettivo

Il perimetro oggettivo comprende ClaimEvidence, le relative interfacce pubbliche e i trattamenti strettamente connessi alle funzionalità descritte. Il sito istituzionale e la libreria documentale sono pubblicati su claimevidence.tech; il servizio applicativo è accessibile sul distinto dominio app.claimevidence.tech. Hostinger fornisce l'infrastruttura e, secondo la configurazione applicabile, il trasporto della posta. MySQL/MariaDB è software eseguito nell'ambiente controllato e non un sub-responsabile autonomo salvo distinto servizio gestito. OpenAI presta il servizio API soltanto per le funzioni abilitate; un eventuale fornitore email separato deve essere identificato e qualificato prima dell'uso.

Le operazioni considerate riguardano raccolta guidata di fotografie e documenti, organizzazione per pratica, controlli di completezza, supporto analitico configurabile, revisione umana ed esportazione. Le categorie di informazioni potenzialmente interessate sono: richieste demo e security pack sul sito; nell'applicazione, identificativi pratica, contatti autorizzati, fotografie, documenti, note, metadati di sessione e output assistiti. L'effettivo ruolo privacy, il titolo giuridico e l'ampiezza del trattamento dipendono dal rapporto contrattuale e dalle istruzioni lecite del soggetto che determina finalità e mezzi essenziali.

Definizioni e criteri interpretativi

- «Servizio»: l'insieme delle funzionalità di ClaimEvidence rese disponibili in base al contratto.
- «Cliente»: la persona giuridica o il professionista che conclude il contratto con Niltech.
- «Utente autorizzato»: la persona fisica abilitata dal Cliente a utilizzare il Servizio sotto la sua responsabilità.
- «Dati del Cliente»: dati, documenti, immagini, istruzioni e ogni altro contenuto conferito o generato per conto del Cliente.

- «Output assistito»: risultato elaborato mediante regole automatizzate o componenti di intelligenza artificiale, soggetto ai controlli indicati.
- «Fornitore ulteriore»: soggetto terzo che presta a Niltech un servizio tecnico rilevante per il perimetro documentato.
- «Incidente»: evento che compromette o può compromettere riservatezza, integrità, disponibilità, autenticità o resilienza.
- «Giorno lavorativo»: ogni giorno diverso da sabato, domenica o festività nazionale italiana.

Obblighi e presidi specifici

1. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a tradurre rischi e requisiti in criteri verificabili di accettazione. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

2. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a proteggere repository, branch, review, pipeline e segreti. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

3. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a analizzare dipendenze, licenze, componenti e vulnerabilità. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

4. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a eseguire test funzionali, security, privacy e regressione proporzionati. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

5. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a rilasciare artefatti identificati con rollback e segregazione. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

6. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a ricevere, valutare, correggere e comunicare vulnerabilità e aggiornamenti. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Ciclo di modifica

Requisiti, progettazione, revisione, test, approvazione, rilascio e rollback sono proporzionati al rischio. Ambienti e accessi sono separati quanto previsto dall’architettura.

Controlli

- validazione input, output encoding e autorizzazione lato server
- gestione segreti e dipendenze senza credenziali nel codice
- test automatici, revisione e scansioni proporzionate
- logging senza dati o segreti non necessari

Vulnerabilità

Le segnalazioni sono validate, classificate per impatto e sfruttabilità, corrette, testate e distribuite con controllo. Le priorità effettive dipendono dal rischio e dalla disponibilità della correzione.

Aggiornamenti e supporto

Componenti supportati, dipendenze, eccezioni e fine supporto sono tracciati nel registro tecnico. Gli obblighi CRA sono valutati per ruolo e qualificazione del prodotto.

Ciclo di vita e sicurezza per progettazione

Requisiti di sicurezza e protezione dati sono definiti prima della modifica, collegati ad asset e minacce, verificati mediante revisione, test e approvazione e mantenuti nel tempo. Le modifiche ad autenticazione, autorizzazione, crittografia, log, upload, elaborazione IA, dipendenze o cancellazione richiedono analisi commisurata all'impatto.

Credenziali e segreti non sono inclusi nel codice o negli artefatti pubblici. Componenti e dipendenze sono inventariati con provenienza e condizioni; vulnerabilità note sono valutate per sfruttabilità e impatto, non soltanto per punteggio astratto.

Cyber Resilience Act e gestione delle vulnerabilità

L'eventuale qualificazione come prodotto con elementi digitali, il ruolo di fabbricante e le esclusioni sono valutati sul prodotto e sul modello di distribuzione. Le principali prescrizioni del Cyber Resilience Act si applicano dall'11 dicembre 2027, mentre gli obblighi di segnalazione previsti dal regolamento si applicano dall'11 settembre 2026. La preparazione comprende classificazione, documentazione, support period, gestione coordinata e canali di reporting, senza dichiarare conformità prima delle evidenze e delle procedure applicabili.

Una vulnerabilità è triaggiata, contenuta, corretta, verificata e comunicata secondo rischio, sfruttamento e obblighi. Le eccezioni hanno owner, motivazione, misura compensativa e scadenza. Correzioni urgenti sono sottoposte a verifica successiva e non eliminano l'analisi della causa.

Ripartizione delle responsabilità e limiti di affidamento

Il Cliente garantisce, per quanto di propria competenza, la liceità dei dati e delle istruzioni conferite, l'abilitazione degli utenti, l'adeguatezza delle basi giuridiche e delle informative, nonché la verifica professionale degli output. Niltech resta responsabile delle attività direttamente poste sotto il proprio controllo e non assume le funzioni regolamentari, deontologiche o decisionali proprie del Cliente.

Gli output di ClaimEvidence hanno natura ausiliaria. Salvo patto espresso e le norme inderogabili, essi non costituiscono parere legale, perizia, decisione assicurativa, determinazione di responsabilità, valutazione creditizia o altro atto riservato. Il destinatario deve esaminare fonti, completezza, coerenza e conseguenze prima di utilizzarli.

Nessuna clausola limita responsabilità che non possa essere esclusa per legge. Fuori da tali ipotesi, imputazione, rimedi, limiti e criteri di quantificazione seguono il contratto applicabile, tenuto conto del concorso del danneggiato, dell'obbligo di mitigazione e della prevedibilità del danno secondo la legge regolatrice.

Prova, riesame, richieste e legge applicabile

Ogni affermazione materiale deve poter essere ricondotta a un contratto, una configurazione approvata, un registro, un verbale, un test, un log o altra evidenza attendibile. Dichiarazioni del fornitore e controlli propri di Niltech sono mantenuti distinti. L'assenza di incidenti non prova, da sola, l'efficacia di una misura.

Le revisioni sono datate, motivate e approvate. Una revisione successiva non modifica retroattivamente i fatti o gli impegni applicabili a periodi precedenti. Le copie pubblicate sono identificate mediante codice, data e impronta crittografica; tali elementi provano l'integrità della copia, non l'efficacia sostanziale dei controlli descritti.

Segnalazioni, richieste di chiarimento, esercizio di diritti e contestazioni possono essere inviati a info@nil-tech.net. Niltech verifica l'identità e la legittimazione quando necessario, registra la richiesta, risponde nei termini applicabili e comunica eventuali proroghe o dinieghi motivati.

Salvo diversa disposizione inderogabile o pattuizione scritta, la legge italiana disciplina l'interpretazione del documento. La versione italiana costituisce il testo di riferimento; la traduzione inglese è fornita per agevolare la consultazione.

Fonti ufficiali e data normativa

Riferimenti verificati al 2026-08-30. L'applicabilità, il ruolo e le eventuali decorrenze devono essere nuovamente accertati sul caso concreto.

- Regolamento (UE) 2016/679 (GDPR)

- Direttiva (UE) 2022/2555 (NIS2)
- D.lgs. 4 settembre 2024, n. 138 — recepimento NIS2 in Italia
- Regolamento (UE) 2024/2847 (Cyber Resilience Act)
- Commissione europea — Quadro di attuazione e scadenze del Cyber Resilience Act, 27 luglio 2026