SECURITY & COMPLIANCE

Scheda del sistema IA e valutazione giuridico-operativa dei rischi

Sistema, pericoli, controlli, rischio residuo e criteri di riesame.

Prodotto	ClaimEvidence
Codice	CLE-PUB-14-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 documentare sistema, contesto, pericoli, persone esposte, controlli, rischio residuo, criteri di accettazione e condizioni di sospensione.

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.

La valutazione ha natura continuativa e documenta scenari di danno, soggetti esposti, misure, efficacia, rischio residuo e decisione. Essa non assegna al prodotto una classe astratta e immutabile: la qualificazione giuridica dipende dall’uso previsto e dalle circostanze concrete.

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 scomporre il sistema in casi d'uso e componenti verificabili. 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 identificare danni da errore, omissione, bias, abuso, dati e indisponibilità. 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 stimare probabilità e impatto con criteri dichiarati. 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 associare controlli preventivi, rilevativi e correttivi a ogni rischio. 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 valutare efficacia con test, campioni, esiti e limiti. 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 accettare, mitigare, evitare o trasferire il rischio con owner e scadenza. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Sistema e contesto

ClaimEvidence: raccolta guidata di fotografie e documenti, organizzazione per pratica, controlli di completezza, supporto analitico configurabile, revisione umana ed esportazione.

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.

Rischi principali

- output inesatti, incompleti o non aggiornati
- eccessivo affidamento e automazione impropria
- dati personali o riservati non necessari
- bias, perdita di contesto o interpretazione errata
- indisponibilità, dipendenza fornitore o uso ostile

Controlli

Uso previsto limitato, avvisi, revisione umana, accessi autorizzati, tracciabilità di fonti e revisioni documentali ove disponibile, gestione fornitori, test e canale incidenti riducono ma non eliminano i rischi.

Rischio residuo e riesame

Il rischio residuo varia da basso ad alto in funzione dei dati e dell'impatto della decisione. Usi con effetti giuridici, finanziari, assicurativi o sui diritti richiedono approvazione, controllo rafforzato e, se necessario, sospensione.

Riesame almeno semestrale e a ogni modifica di modello, provider, finalità, categoria dati, incidente o requisito.

Conclusione di classificazione condizionata

La raccolta e organizzazione di evidenze di sinistro e il supporto alla revisione non determinano, in quanto tali, copertura, responsabilità o liquidazione e non sono qualificati in via astratta come impiego ad alto rischio. La classificazione deve essere riaperta se il sistema viene destinato a decidere o raccomandare autonomamente esiti che producono effetti giuridici o analogamente significativi.

La conclusione vale esclusivamente per l'uso previsto descritto, con output ausiliario e revisione umana effettiva. Non è un'attestazione permanente: una modifica sostanziale o una nuova finalità può mutare ruolo, categoria di rischio e obblighi.

Scenari di danno e soggetti incisi

La valutazione considera utenti, persone menzionate nei fascicoli, clienti, controparti, professionisti e terzi. Il rischio non è ridotto al malfunzionamento tecnico: comprende discriminazione, perdita di riservatezza, errore professionale, pregiudizio economico, mancata possibilità di contestazione e uso del risultato fuori contesto.

- omissione o erronea classificazione di una prova, con falsa percezione di completezza
- metadati, volti, targhe o terzi acquisiti oltre quanto necessario
- eccessivo affidamento sull'output, automation bias o mancata escalation dell'incertezza
- indisponibilità, dipendenza da fornitore, attacco o manipolazione di input e istruzioni

Metodo, rischio residuo e decisione

Per ogni scenario il registro controllato identifica causa, evento, danno, soggetto inciso, probabilità e gravità con scala definita, controlli preventivi e rilevativi, test, owner e rischio residuo. Un controllo è accreditato soltanto se applicabile al perimetro e sostenuto da prova; la mera previsione documentale non riduce il rischio.

Il rischio residuo è accettato, mitigato, trasferito o conduce a divieto/sospensione da parte di un soggetto con autorità adeguata. Non è formulata in questo documento una valutazione numerica o una conclusione di accettabilità priva del fascicolo delle evidenze.

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) 2024/1689 (AI Act)
- Regolamento (UE) 2026/1744 — Omnibus digitale sull'IA
- Commissione europea — Linee guida finali sugli obblighi di trasparenza dell'articolo 50 AI Act, luglio 2026
- Regolamento (UE) 2016/679 (GDPR)

Controllo del documento: la copia identificata nel manifest mediante impronta SHA-256 costituisce l'edizione documentale pubblicata alla data indicata. Il sigillo in intestazione è un elemento grafico societario neutro e non costituisce firma digitale, attestazione di terza parte o certificazione.