



SECURITY & COMPLIANCE

Business continuity, backup e disaster recovery

Governance della continuità senza obiettivi o capacità non provati.

Prodotto	Context
Codice	CTX-PUB-19-IT
Edizione documentale	Edizione del 27 luglio 2026
Efficacia / riesame	2026-07-27 / 2027-01-27
Titolare del documento	Niltech Europe S.r.l. · Compliance & Security
Classificazione	Pubblico

Preambolo, natura ed efficacia del documento

Niltech Europe S.r.l., con sede legale in Via Calmaggione 5, 31100 Treviso (TV), Italia, P. IVA IT 05614380268 (di seguito «Niltech»), adotta il presente documento al fine di descrivere governance di continuità, backup e ripristino distinguendo principi pubblici da valori e configurazioni riservati verificati.

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 continuità è governata secondo un approccio proporzionato a servizi, dati e dipendenze. Obiettivi temporali o di perdita dati acquistano valore impegnativo soltanto se concordati nel contratto o approvati in un piano corredato da prove di ripristino.

Ambito soggettivo e oggettivo

Il perimetro oggettivo comprende Context, le relative interfacce pubbliche e i trattamenti strettamente connessi alle funzionalità descritte. Il sito e il servizio Context sono destinati al dominio contextai.legal e utilizzano infrastruttura Bluehost. OpenAI presta servizi di elaborazione IA; MySQL, Redis, ClamAV, Tesseract, Poppler, ImageMagick ed Exim/sendmail sono componenti tecnici gestiti nell'ambiente del servizio e non sono, per ciò solo, sub-responsabili autonomi. Le funzioni di ricerca giuridica, quando abilitate dal cliente e pertinenti alla richiesta, possono interrogare fonti pubbliche istituzionali, tra cui Cassazione/SentenzeWeb, Normattiva, AGCM e ANAC; la provenienza istituzionale non esonera l'utilizzatore dalla verifica dell'aggiornamento, della pertinenza e del testo ufficiale applicabile.

Le operazioni considerate riguardano caricamento e classificazione documenti, estrazione testo e OCR, analisi e sintesi assistite, redazione di report, revisione e ricerca giuridica su fonti abilitate. Le categorie di informazioni potenzialmente interessate sono: account autorizzati, fascicoli, documenti, testo estratto, risultati OCR, note, fonti giuridiche, log operativi 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 Context 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 senza pregiudizio per le responsabilità del Cliente, provvede a identificare processi critici, dipendenze, owner e scenari. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
2. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a svolgere analisi d'impatto e priorità approvate. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
3. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a inventariare backup, protezioni, retention e responsabilità. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
4. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a provare ripristini in ambiente isolato e verificarne integrità. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
5. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a coordinare comunicazioni, workaround e ritorno controllato. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
6. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a riesaminare piano e dipendenze dopo test, incidente o cambiamento. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.

Ambito

Il sito e il servizio Context sono destinati al dominio contextai.legal e utilizzano infrastruttura Bluehost. OpenAI presta servizi di elaborazione IA; MySQL, Redis, ClamAV, Tesseract, Poppler, ImageMagick ed Exim/sendmail sono componenti tecnici gestiti nell'ambiente del servizio e non sono, per ciò solo, sub-responsabili autonomi. Le funzioni di ricerca giuridica, quando abilitate dal cliente e pertinenti alla richiesta, possono interrogare fonti pubbliche istituzionali, tra cui Cassazione/SentenzeWeb, Normattiva, AGCM e ANAC; la provenienza istituzionale non esonera l'utilizzatore dalla verifica dell'aggiornamento, della pertinenza e del testo ufficiale applicabile.

Servizi critici, dipendenze, dati e responsabili sono censiti nel piano controllato.

Strategie

- backup secondo calendario approvato e separazione logica ove disponibile
- procedure di ripristino e controlli di integrità
- continuità manuale o degradata per funzioni prioritarie
- contatti, escalation, comunicazione e dipendenze fornitore

Test

Il valore di un backup è dimostrato da ripristini verificati. Esiti, lacune e azioni sono registrati. Frequenze e obiettivi sono stabiliti nel contratto o nel piano approvato, non in questa sintesi pubblica.



Evento di continuità

Si attivano triage, contenimento, decisione di failover o ripristino, comunicazioni, verifica dei dati e ritorno controllato al servizio. Gli obblighi di notifica sono valutati separatamente.

Ambito, destinatari e valore del documento

Questo documento è destinato a clienti, prospect, utenti autorizzati, consulenti e funzioni di controllo che devono comprendere il perimetro di Context. Il suo obiettivo specifico è descrivere governance di continuità, backup e ripristino distinguendo principi pubblici da valori e configurazioni riservati verificati. La descrizione si applica alla revisione documentale e alla data indicate e deve essere letta insieme a contratto, ordine, DPA, specifiche tecniche e procedure controllate applicabili.

Il sito e il servizio Context sono destinati al dominio contextai.legal e utilizzano infrastruttura Bluehost. OpenAI presta servizi di elaborazione IA; MySQL, Redis, ClamAV, Tesseract, Poppler, ImageMagick ed Exim/sendmail sono componenti tecnici gestiti nell'ambiente del servizio e non sono, per ciò solo, sub-responsabili autonomi. Le funzioni di ricerca giuridica, quando abilitate dal cliente e pertinenti alla richiesta, possono interrogare fonti pubbliche istituzionali, tra cui Cassazione/SentenzeWeb, Normattiva, AGCM e ANAC; la provenienza istituzionale non esonera l'utilizzatore dalla verifica dell'aggiornamento, della pertinenza e del testo ufficiale applicabile.

In caso di divergenza prevalgono gli accordi sottoscritti e le configurazioni effettivamente approvate. Le informazioni pubbliche descrivono il programma di controllo e non trasformano capacità opzionali dei provider in controlli Niltech, né attestano automaticamente l'applicabilità o il soddisfacimento di una norma.

Definizioni operative

Le definizioni seguenti servono a interpretare il documento in modo coerente. I termini definiti dalla legge o dal contratto mantengono il significato attribuito dalla relativa fonte.

- Servizio critico: funzione la cui indisponibilità produce un impatto materiale sul cliente.
- Continuità: capacità organizzativa di mantenere o ripristinare attività prioritarie durante un evento.
- Backup: copia protetta destinata al ripristino e distinta da replica o alta disponibilità.
- Ripristino: recupero controllato di dati e servizi seguito da verifiche di integrità e funzionalità.
- Scenario: evento plausibile usato per pianificare risposta, comunicazioni, risorse e dipendenze.

Requisiti e processo operativo

Il processo deve rimanere proporzionato al caso d'uso, ai dati, alle persone esposte e al possibile impatto. Per Context, le funzioni rilevanti comprendono caricamento e classificazione documenti, estrazione testo e OCR, analisi e sintesi assistite, redazione di report, revisione e ricerca giuridica su fonti abilitate. Ogni fase deve avere un responsabile, input verificabili, criteri di completamento, evidenze e un percorso di escalation.

Prima dell'attivazione o della pubblicazione, l'owner verifica che i requisiti siano tradotti in controlli concreti e che i controlli siano effettivamente applicabili all'ambiente. Un controllo solo pianificato, una capacità non configurata o una dichiarazione generale del fornitore sono registrati come gap e non come misura operativa.

- identificare processi critici, dipendenze, owner e scenari
- svolgere analisi d'impatto e priorità approvate
- inventariare backup, protezioni, retention e responsabilità
- provare ripristini in ambiente isolato e verificarne integrità
- coordinare comunicazioni, workaround e ritorno controllato
- riesaminare piano e dipendenze dopo test, incidente o cambiamento

Ruoli e responsabilità

Niltech mantiene il documento, le configurazioni sotto il proprio controllo e il collegamento alle evidenze. Il cliente determina finalità, utenti, dati, autorizzazioni e decisioni professionali nel proprio perimetro. I provider rispondono delle componenti definite dai rispettivi contratti. I destinatari principali del prodotto sono professionisti legali e organizzazioni che analizzano fascicoli, documenti e fonti giuridiche.

Nessun ruolo è attribuito implicitamente. Owner di prodotto, sicurezza, privacy, continuità e IA devono essere identificati nel registro controllato. Quando una persona ricopre più ruoli, l'approvazione di rischi, eccezioni o risultati materiali deve



includere una verifica indipendente proporzionata.

- Direzione: approva rischio residuo, eccezioni materiali e priorità.
- Owner: mantiene requisiti, controlli, evidenze, gap e riesami.
- Operatori: seguono istruzioni, verificano input/output e segnalano anomalie.
- Cliente: assicura liceità, autorizzazioni, qualità dei dati e uso professionale.
- Fornitori: erogano i servizi e le informazioni previste dai relativi accordi.

Evidenze, verifiche e accountability

Ogni affermazione materiale deve essere riconducibile a un'evidenza corrente: configurazione, contratto, report, test, ticket, verbale, log o registro. Le evidenze sono classificate, accessibili solo a chi ne ha necessità e conservate secondo il calendario applicabile. Hash e revisione documentale identificano i documenti, ma non provano da soli l'efficacia di un controllo.

La verifica valuta esistenza, pertinenza, copertura, data, risultato e limiti dell'evidenza. Campioni e test devono essere rappresentativi del rischio dichiarato. Esiti negativi o parziali generano un'azione con owner e scadenza; non sono omessi dalla sintesi quando incidono sulla comprensione del rischio.

- business impact analysis e inventario dipendenze
- piani di continuità, comunicazione e ripristino
- inventario backup e prove di ripristino isolate
- test di scenario, risultati, gap e remediation
- incidenti, decisioni di attivazione e lessons learned

Salvaguardie trasversali

Privacy, sicurezza, qualità e continuità sono considerate in ogni fase e non soltanto al termine. I dati sono limitati a quanto necessario; accessi e autorizzazioni seguono il minimo privilegio; modifiche e attività amministrative sono tracciate in misura proporzionata; input, trasformazioni e output mantengono una provenienza sufficiente alla verifica professionale.

Dati particolari, informazioni altamente riservate, minori o persone vulnerabili richiedono una valutazione specifica prima del trattamento. Quando il controllo necessario non è disponibile o non è provato, si riduce il perimetro, si applica una modalità manuale, si rimuove il dato o si sospende il caso d'uso.

- minimizzazione di dati, campi liberi, prompt, log ed export
- accesso nominativo, segregazione dei ruoli e revoca tempestiva
- validazione di formato, integrità, completezza e provenienza
- protezione di trasporto, copie di lavoro e canali di condivisione secondo evidenza
- modalità degradata, escalation e comunicazione quando dipendenze o controlli non sono disponibili

Eccezioni, non conformità ed escalation

Uno scostamento non è accettato per consuetudine. L'owner registra requisito interessato, causa, impatto, dati e persone esposte, misure compensative, approvatore, scadenza e criterio di chiusura. L'eccezione è riesaminata se cambia il rischio o se una misura non produce l'effetto previsto.

Devono essere escalati senza ritardo incidenti, possibile trattamento illecito, perdita di controllo sui dati, output con impatto grave, violazioni contrattuali, fornitore non approvato o evidenza inattendibile. Ai fini del presente documento si considera quanto segue: Il perimetro documentato comprende sito, servizio applicativo, componenti tecnici e fonti esterne utilizzate secondo contratto.

- contenere il rischio e sospendere la fase interessata quando necessario
- preservare prove, orari, decisioni e comunicazioni
- coinvolgere owner privacy, sicurezza, prodotto, legale o direzione secondo il caso
- riattivare solo dopo verifica della misura e autorizzazione documentata



Riesame, modifiche e miglioramento

Il documento è riesaminato almeno semestralmente e prima quando cambiano finalità, destinatari, dati, ruolo GDPR o AI Act, provider, modello, architettura, localizzazione, termini contrattuali o requisiti normativi. Incidenti, reclami, test falliti e nuove vulnerabilità attivano un riesame straordinario.

Ogni revisione registra input, partecipanti, decisione, modifiche, evidenze sostituite, gap residui e data successiva. Correzioni materiali sono pubblicate senza alterare retroattivamente la revisione documentale precedente. Contatti e richieste: info@nil-tech.net.

- verifica del registro modifiche e dei documenti collegati
- nuovo test dei controlli interessati
- aggiornamento di manifest, PDF, HTML e hash
- comunicazione ai destinatari quando la modifica incide sui loro diritti o obblighi

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 Context 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 2026-07-27. 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) e stato di attuazione in Italia
- Regolamento (UE) 2022/2554 (DORA)

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.