NIS2 per i fornitori

Stay in the Chain

Guida pratica per vendor e fornitori che servono clienti soggetti a NIS2 o a requisiti analoghi di sicurezza della supply chain

Come usare questa guida

Questa guida è pensata per fornitori che non sono necessariamente regolati direttamente da NIS2, ma lavorano per clienti che rientrano tra le entità essenziali o importanti della Direttiva, oppure per clienti che applicano requisiti di sicurezza della supply chain per ragioni contrattuali, di gruppo o di settore. Non promette conformità legale. Aiuta i fornitori a costruire un pacchetto di evidenza strutturato che il cliente possa valutare, archiviare e difendere internamente.

In questo documento, dossier e pacchetto di evidenza indicano la stessa cosa: un insieme ordinato di file, registri, report, dichiarazioni, screenshot, procedure, manifest e attestazioni collegati a uno specifico perimetro di servizio o a una richiesta del cliente.

Questa guida è uno strumento metodologico e operativo, non un parere legale e non una certificazione di conformità. L'applicabilità diretta di NIS2 a un fornitore, gli obblighi concreti, le scadenze, le autorità competenti e le conseguenze giuridiche devono essere valutati caso per caso sulla base del recepimento nazionale applicabile, dei contratti con il cliente e del ruolo effettivo del fornitore nella catena di fornitura.

La promessa pratica è semplice: non vendere "conformità NIS2", ma aiutare il fornitore a diventare più facile da qualificare, più leggibile e più difendibile davanti a clienti regolati o comunque sottoposti a requisiti di sicurezza della supply chain.

- Usa la Parte I per comprendere il cambio di mentalità commerciale e operativa.
- Usa la Parte II per comprendere l'infrastruttura di evidenza: manifest, hash, Census, integrazione SDK/API e posizionamento CertiSigma.
- Usa la matrice qui sotto per individuare il playbook settoriale più vicino al tuo caso.
- Usa ogni playbook per costruire un pacchetto di evidenza proporzionato a una specifica relazione cliente-fornitore.
- Usa la Parte IV per posizionare il lavoro commercialmente senza dichiarare più di quanto puoi dimostrare.

Trova il tuo playbook

Se...	Parti da questo playbook
Installi dispositivi dentro reti o ambienti del cliente	Installatori di sistemi connessi
Gestisci cloud, utenti, backup o strumenti di security	MSP, consulenti IT e system integrator
Sviluppi, ospiti o mantieni piattaforme software	Software house, SaaS provider e agenzie web tecniche
Intervieni su macchine, PLC o linee produttive	Manutentori tecnici, OT e macchinari industriali
Tratti documenti legali, fiscali, payroll, amministrativi o tecnici	Studi professionali e document management provider
Gestisci spedizioni, WMS, tracking o fulfilment	Logistica, magazzino e trasporti
Gestisci edifici, badge, CCTV o BMS	Facility management e building services
Gestisci pazienti, dati di cura o continuità clinica	Sanità, assistenza e servizi alla persona
Gestisci negozi, pagamenti, CRM, POS o marketplace	Retail, e-commerce e servizi digitali B2B
Gestisci studenti, LMS, device condivisi o piattaforme formative	Scuole, formazione e istituzioni educative
Gestisci donatori, volontari, cloud, progetti o grant	Associazioni, fondazioni e non-profit strutturate
Accedi fisicamente per eventi, test, lavori temporanei o audit	Accesso fisico-operativo, eventi e system testing

Parte I: realtà, mentalità, framework

1. Il vero innesco: non la legge, ma il cliente

Per molte piccole e medie imprese, NIS2 non arriverà come Direttiva europea, circolare ministeriale o memo legale. Arriverà come email di un cliente:

> *Gentile fornitore, nell'ambito delle nostre attività di gestione del rischio e sicurezza della supply chain previste da NIS2, vi chiediamo di compilare il questionario allegato e di fornire evidenza documentale su cybersecurity, controllo degli accessi, gestione degli incidenti, continuità operativa e subfornitori.*

È lì che comincia la sfida. La tua azienda potrebbe non essere direttamente in ambito. Potresti non gestire infrastrutture critiche, ospedali, piattaforme finanziarie o servizi digitali essenziali. Potresti essere un installatore, un MSP, uno sviluppatore software, un consulente tecnico, un facility contractor, un partner logistico, uno studio professionale o un event provider.

Eppure, improvvisamente, ti trovi dentro il perimetro. Non perché il regolamento ti nomini direttamente, ma perché il tuo cliente deve dimostrare controllo sulla propria supply chain. NIS2 richiede alle essential e important entities di trattare la sicurezza della supply chain come parte delle misure di cybersecurity risk management, includendo i rischi collegati a fornitore e service provider.

La trasformazione pratica è chiara: la cybersecurity non resta più confinata nell'dipartimento IT del cliente. Scende lungo la catena. Raggiunge chi installa, mantiene, configura, accede, sviluppa, archivia, processa o supporta servizi operativi.

La domanda utile non è più: siamo soggetti a NIS2? La domanda più realistica è: quando un cliente soggetto a NIS2 ci chiede prova, sappiamo rispondere in modo chiaro?

2. Che cosa significa davvero NIS2

NIS2 aggiorna il quadro europeo per la sicurezza delle reti e dei sistemi informativi. Estende i settori coperti, rafforza il risk management, impone obblighi di incident reporting, attribuisce responsabilità agli organi di gestione e dà peso esplicito alla sicurezza della supply chain.

Tradotto in termini operativi, NIS2 dice una cosa molto semplice: le organizzazioni importanti per funzioni sociali ed economiche devono gestire la cybersecurity come disciplina strutturata, non come pensiero successivo.

- Quali rischi affrontano

- Quali sistemi utilizzano
- Quali fornitori toccano i loro processi
- Chi accede ai loro dati o alla loro infrastruttura
- Come gestiscono incidenti, backup, continuità operativa, vulnerabilità e subfornitori
- Quale evidenza possono produrre in caso di audit, incidente o controllo regolatorio

Per un fornitore questo non significa diventare una multinazionale della conformità. Significa rispettare una regola pratica: se tocchi qualcosa di importante per il cliente, devi poter spiegare che cosa tocchi, come lo tocchi, chi lo tocca, con quali regole, con quali limiti e con quale evidenza.

Il risultato non è una dichiarazione di conformità NIS2. È un dossier strutturato e proporzionato di evidenza verificabile.

3. Perimetro legale ed esposizione commerciale

Questa è la distinzione decisiva: un fornitore può essere fuori perimetro dal punto di vista legale e allo stesso tempo esposto commercialmente.

Potresti non avere obblighi diretti verso il regolatore. Potresti però dover fornire evidenza al cliente. Per questo la pressione NIS2 indiretta conta. La relazione commerciale diventa il canale di enforcement. Il cliente invia il questionario, l'approvvigionamento chiede evidenza, il contratto aggiunge clausole, l'audit domanda documentazione e il fornitore deve rispondere.

Il fornitore che tratta questa dinamica come un fastidio risponde tardi, in modo vago e difensivo. Il fornitore che la interpreta come segnale di mercato prepara un pacchetto di evidenza riutilizzabile e diventa più facile da qualificare.

4. Perché i fornitori sentono NIS2 prima che si applichi a loro

Lo senti perché non hai avviato tu il processo. Lo ha avviato il cliente. Il cliente manda il questionario. Il cliente chiede prova su MFA, elenco accessi, log di accesso remoto, mappa dei subfornitori, piano di continuità e procedure di incidente.

La reazione naturale è frustrazione: un altro modulo, un'altra richiesta burocratica, un altro cliente che chiede prova di attività che già svolgi. È una reazione comprensibile. Molti fornitori lavorano bene da anni. La fiducia si è costruita su reputazione, prontezza e competenza concreta.

Però, nelle supply chain regolate, la fiducia informale non basta più. Il cliente non può più limitarsi a dire: lavoriamo con loro da anni. Deve poter dire: gli accessi sono

controllati, gli interventi sono registrati, le configurazioni sono documentate, l'evidenza è disponibile e i limiti sono dichiarati.

NIS2 non elimina la fiducia. Le chiede di lasciare traccia. Per i fornitori competenti, questo non è una minaccia. È un'opportunità.

5. L'equivoco centrale: diventare «conformi a NIS2»

Il primo errore è pensare di dover diventare conforme a NIS2. Per molti fornitori indiretti, questa formula è imprecisa e rischiosa.

Un fornitore indiretto non deve inventarsi certificazioni, comprare GRC platform sovradimensionate o copiare policy che non è in grado di applicare. Deve rispondere in modo credibile a un cliente che ha responsabilità legale.

- Chiarire con il cliente il perimetro del servizio
- Identificare sistemi, dati, punti di accesso e responsabilità toccati dal servizio
- Raccogliere l'evidenza già esistente
- Creare la documentazione minima mancante
- Mappare ogni elemento di evidenza a una richiesta del cliente
- Dichiarare i limiti in modo esplicito
- Tenere aggiornato il dossier
- Dimostrare esistenza, versione e data dei file quando rilevante

Questa è la logica del Dossier di evidenza per il fornitore NIS2. Non vende conformità immaginaria. Costruisce una lingua comune con il cliente.

6. Parlare la lingua del rischio del cliente

Un cliente soggetto a NIS2 non valuta più i fornitori solo su prezzo, consegna e qualità. Valuta anche l'esposizione al rischio.

- Questo fornitore può introdurre rischio nei nostri sistemi?
- Accede ai nostri dati o alla nostra infrastruttura?
- Può interrompere un processo critico?
- Introduce vulnerabilità non corrette?
- Condivide credenziali o lascia accessi remoti aperti?
- Può subire un incidente e non notificarcelo?
- Usa subfornitori che non conosciamo?
- In caso di audit, possiamo dimostrare di averlo valutato?

Le rassicurazioni generiche non sono evidenza. Sono opinioni. Parlare la lingua del cliente significa rispondere con perimetro del servizio, confini, sistemi e dati toccati, personale autorizzato, strumenti e controlli di accesso, procedure di incidente e continuità operativa, subfornitori rilevanti, evidenza disponibile, limiti dichiarati e manifest dei file.

7. Perché non è solo burocrazia

Liquidare NIS2 come burocrazia è comodo, ma miope. Le organizzazioni moderne, le infrastrutture critiche e le supply chain dipendono da sistemi digitali interconnessi. Un cyber incident non è più solo un problema IT. Può fermare la produzione, ritardare consegne, interrompere cure, bloccare pagamenti, compromettere la safety e generare penali contrattuali.

Il rischio cyber è rischio operativo. Il rischio operativo non si ferma ai confini aziendali. Viaggia attraverso credenziali condivise, accesso remoto, software privo di patch, backup non documentati, account non revocati, subfornitori opachi e manutenzione non tracciata.

Una buona documentazione non produce carta vuota. Rende visibile il lavoro reale. Per i fornitori competenti, questo diventa un vantaggio commerciale.

8. Trasformare il lavoro invisibile in valore visibile

Molti fornitori fanno già le cose giuste: cambiano credenziali predefinite, configurano controllo degli accessi, aggiornano firmware, gestiscono backup, conoscono gli ambienti cliente, risolvono incidenti, mantengono sistemi, proteggono documentazione, intervengono fuori orario e tengono in piedi infrastrutture complesse.

Questo lavoro, però, spesso resta invisibile. Vive nella testa dei tecnici, in chat sparse, cartelle disordinate, screenshot senza data o file chiamati final_v3_revised_OK.pdf.

NIS2 costringe questo lavoro a emergere. Quando emerge, diventa valore. Un fornitore che produce evidenza ordinata sta dicendo: fidatevi di noi perché possiamo mostrare come lavoriamo.

Non serve la perfezione. Serve leggibilità. Un fornitore leggibile è più facile da valutare, spiegare internamente e difendere in audit. Un fornitore difendibile resta nella supply chain.

9. Il nuovo criterio competitivo: essere facili da qualificare

Prima, competitività significava costo, rapidità e uptime. Contano ancora. Per i clienti soggetti a NIS2 o a requisiti analoghi di sicurezza della supply chain, però, emerge un nuovo criterio: quanto è facile qualificarti come fornitore a basso rischio?

Se il cliente deve inseguirti per settimane, interpretare risposte vaghe, coinvolgere legal e IT e resta comunque senza elenco accessi o incident procedure, assocerà il tuo nome al rischio. Se rispondi con un dossier strutturato, mandi un segnale diverso: non saremo il vostro problema di conformità.

In termini di supply chain, questo è un vantaggio competitivo. Non perché hai comprato la piattaforma più costosa, ma perché sei preparato. Hai un perimetro, contatti nominativi, evidenza, un manifest, version control, limiti dichiarati e una struttura.

10. Cinque leve commerciali in NIS2

Differenziazione: quando i concorrenti sembrano simili, un'evidenza ordinata diventa un fattore distintivo.

Riduzione dell'attrito: risposte strutturate accelerano approvvigionamento, rinnovi, onboarding e audit.

Protezione contrattuale: molti fornitori perderanno clienti non per scarso servizio, ma per processi non documentati.

Accesso al mercato: una documentazione chiara apre porte verso imprese più grandi, settori regolati e partner internazionali.

Resilienza interna: preparare l'evidenza costringe a chiarire accessi, procedure, incidenti, backup e ownership.

11. Non ti serve tutto. Ti serve ciò che conta

Un errore frequente è pensare che il dossier debba contenere tutto. Così si crea paralisi. Il dossier deve essere proporzionato al servizio e alla relazione con il cliente.

Accesso remoto? Documentalo.

Tratti dati? Specifica quali e come.

Installi dispositivi connessi? Documenta firmware, credenziali, rete e manutenzione.

Consegni software? Copri release, vulnerabilità, ambienti, backup e accesso alla produzione.

Il tuo servizio può bloccare il cliente? Affronta la continuità operativa.

Usi subfornitori critici? Dichiarali.

La maturità non consiste nel fingere di avere tutto. Consiste nel sapere cosa è rilevante e nel dichiarare cosa non lo è.

12. Dai documenti generici all'evidenza verificabile

Il vecchio modo di rispondere si basava su PDF allegati, policy generiche, screenshot sparsi, file senza data, versioni confuse e cartelle disorganizzate. Il nuovo modo collega ogni elemento di evidenza a una richiesta, identifica e data i file, mantiene l'integrità e usa un manifest che elenca contenuti, versioni, date e hash.

Dove opportuno, integrity attestazioni o timestamp possono rafforzare il package. Una cartella casuale diventa così una catena verificabile: request -> evidenza -> file -> hash -> manifest -> attestation -> client dossier.

Non certifica la perfezione. Rende il pacchetto documentale auditable. Nei contesti NIS2, la verificabilità pesa.

13. La differenza tra dichiarare e dimostrare

Molte organizzazioni sanno dichiarare. Dichiarano attenzione alla sicurezza, esperienza, fiducia dei clienti e affidabilità storica. Quando arrivano richieste NIS2, però, le dichiarazioni non bastano.

Abbiamo backup -> report di backup datato

Usiamo MFA -> policy ed export di configurazione che mostrano lo stato MFA

Gli accessi sono gestiti -> elenco accessi con ruoli, privilegi e data dell'ultima review

Rispondiamo rapidamente agli incidenti -> procedura con contatti, escalation e tempi di notifica

Questo documento esisteva già -> hash, manifest e timestamp

NIS2 per i fornitori indiretti è il passaggio dalla narrazione alla dimostrazione. La narrazione premia chi parla bene. L'evidenza premia chi opera in modo ordinato.

14. La paura dei piccoli fornitori: non siamo strutturati

Molti piccoli fornitori pensano di essere troppo piccoli per questo. Proprio per questo serve un approccio diverso.

Non serve una suite GRC enterprise, controlli astratti o gergo da CISO. Serve un metodo semplice per capire quali richieste del cliente si applicano, raccogliere evidenza minima ma rilevante e presentarla in modo ordinato e verificabile.

Una piccola impresa non deve diventare un dipartimento conformità. Deve diventare un fornitore leggibile. I dipartimenti conformità creano burocrazia interna. I fornitori leggibili costruiscono fiducia esterna.

15. Il cambio culturale: smettere di lavorare a memoria

Le PMI spesso lavorano a memoria: lo sa Luca, è sul laptop di Marco, era nella mail di marzo, se lo ricorda il tecnico.

Funziona fino a quando un incidente, un turnover, una richiesta urgente, un audit o una richiesta di un grande cliente espone il vuoto. La memoria è preziosa, ma non è un sistema.

Un dossier di evidenza trasforma la memoria operativa in asset organizzativo. Non sostituisce l'esperienza. La conserva. Se Luca se ne va o Marco non è disponibile, l'azienda non riparte da zero. Ha una baseline.

16. Che cosa non dire a un cliente soggetto a NIS2

Alcune risposte generano più rischio che fiducia. Evita overclaim e rassicurazioni vaghe.

- Siamo conforme a NIS2, se non sei stato valutato o certificato direttamente.
- Non abbiamo mai avuto problemi.
- Se ne occupa il nostro provider.
- La sicurezza è importante per noi.
- Lo sa il tecnico.
- È tutto nel cloud.
- Possiamo mandare screenshot se serve.

Sostituiscile con linguaggio di evidenza concreto:

- Ecco il nostro service perimeter.
- Ecco la elenco accessi.
- Ecco il report di backup.
- Ecco i subfornitori coinvolti.
- Ecco i limiti della nostra responsabilità.
- Ecco il manifest dei file.

17. NIS2 come grammatica della fiducia

NIS2 introduce una nuova grammatica. Non basta più dire fidatevi. La nuova grammatica è: ecco il perimetro, ecco le responsabilità, ecco gli controllo degli accessi, ecco le misure, ecco l'evidenza, ecco i limiti, ecco il manifest, ecco quando questi file esistevano ed ecco che cosa possiamo dimostrare.

Può sembrare freddo, ma rafforza la fiducia. La fiducia informale dipende dalle persone. La fiducia documentata resiste al cambiamento. La fiducia verificabile può essere condivisa con approvvigionamento, IT, legal, management, auditor, insurer e partner.

Per i fornitori, NIS2 è un invito a diventare più presentabili, più resilienti e più selezionabili. Non in modo cosmetico. Operativamente.

18. La promessa del Quadro di evidenza

Il Quadro di evidenza per il fornitore NIS2 nasce da un'idea semplice: la maggior parte dei fornitori non ha bisogno di una cattedrale di governance tools. Ha bisogno di una valigetta ordinata.

- Chi siamo
- Che cosa consegniamo
- Che cosa tocchiamo
- Chi accede
- Quali dati trattiamo
- Quali sistemi usiamo
- Quali subfornitori coinvolgiamo
- Quali procedure minime seguiamo
- Quale evidenza possiamo mostrare
- Quali file compongono il dossier
- Quali limiti dichiariamo
- Quali integrity measures rafforzano la verificabilità

Il valore sta nella semplificazione senza svuotamento. Il quadro dice: organizza quello che fai, dichiara quello che non fai, dimostra quello che puoi dimostrare.

19. Conclusione: chi sa rispondere resta nella chain

NIS2 non avrà lo stesso impatto su tutti. Alcune entità avranno obblighi diretti. Altre sentiranno pressione indiretta. Alcune vedranno solo richieste occasionali. Una tendenza, però, è chiara: i clienti strutturati chiederanno sempre più evidenza ai fornitori.

Lo faranno perché il rischio cyber è ormai rischio di supply chain. In una supply chain regolata, un fornitore opaco diventa un rischio. Un fornitore ordinato diventa soluzione.

Per i fornitori indiretti, NIS2 può diventare una grande opportunità: differenziarsi, proteggere contratti, accedere a clienti più grandi, fare ordine, trasformare file dispersi in evidenza, rendere visibile il lavoro ben fatto e passare dalla rassicurazione alla prova.

L'obiettivo non è dichiarare conformità per marketing. L'obiettivo è diventare dimostrabilmente affidabili. Nel mercato che emerge, questo può essere il discrimine tra chi resta nella supply chain e chi viene progressivamente sostituito.

Parte II: l'infrastruttura di evidenza

1. Dal panico da questionario alla risposta basata su evidenza

Una richiesta del cliente non è sempre scritta bene. Alcuni clienti chiederanno una certificazione NIS2 anche quando non esiste un certificato fornitore per quel perimetro di servizio. Altri invieranno un questionario pensato per un'impresa regolata, non per un installatore, MSP, partner logistico, scuola, studio professionale o event provider.

Il fornitore non deve overclaimare e non deve rifiutare la richiesta in modo difensivo. La risposta pratica è tradurre la domanda in perimetro, evidenza e limiti.

Una risposta sicura è: non stiamo rivendicando una certificazione NIS2. Possiamo fornire un dossier di evidenza strutturato per i servizi che eroghiamo a vostro favore, includendo file rilevanti, limiti dichiarati, confini di responsabilità e manifest.

Il fornitore deve distinguere con chiarezza ciò che gestisce, ciò che non gestisce, ciò che dipende dal cliente, ciò che dipende da terzi, ciò che è già dimostrabile e ciò che richiederebbe attività tecnica o legale aggiuntiva.

2. Livelli di maturità dell'evidenza

Il percorso non deve partire dalla crittografia avanzata. Un piccolo fornitore non dovrebbe sentirsi costretto a saltare dalle cartelle informali a un ciclo di vita dell'evidenza sofisticato. Il quadro può essere adottato per livelli.

Level 1 - Pacchetto di evidenza base: perimetro del servizio, contatto nominativo, file chiave, checklist semplice, limiti dichiarati e file list datata. Adatto alla prima richiesta cliente o a un fornitore a rischio basso.

Level 2 - Structured Dossier: evidenza mappata sulle domande del cliente, elenco accessi, registri, subfornitori, contatti per incident, report di backup e file versionati. Adatto a clienti ricorrenti e questionari per i fornitori.

Level 3 - Verifiable Dossier: manifest, hash, versioni dei file, timestamp o riferimenti di attestazione, e una catena chiara che collega request, file, hash, manifest ed evidenza. Adatto a fornitori critici, audit e contratti di valore elevato.

Level 4 - Managed Evidence Process: revisioni periodiche, automated file census, integrazione SDK/API, attestazioni ricorrenti e lifecycle management. Adatto a MSP, SaaS provider, OT maintainer, healthcare provider, platform e fornitori più grandi.

Il punto è anche commerciale. Hash e attestazioni sono potenti, ma non vanno presentati come un peso da day one. Il primo passo è sapere esattamente cosa è stato

inviato, quando, per quale cliente e con quale scopo. Il passo avanzato è rendere quel pacchetto tecnicamente verificabile.

3. Perché il dossier ha bisogno di una spina dorsale tecnica

Un dossier di evidenza strutturato è utile solo se può essere mantenuto, versionato e verificato. Altrimenti resta l'ennesima cartella di PDF, screenshot, export e report.

Qui molti piccoli fornitori falliscono. Possono avere i file giusti, ma non la struttura di evidenza corretta. I file vengono rinominati, sovrascritti, copiati, inviati via e-mail, salvati in cartelle diverse o aggiornati senza una traccia chiara. Quando il cliente chiede, il fornitore sa forse che l'evidenza esiste, ma non quale versione è stata inviata, quando esisteva, se è cambiata o come si collega alla richiesta cliente.

Lo strato mancante non è un'altra piattaforma GRC pesante. Lo strato mancante è una infrastruttura leggera di evidenza.

4. CertiSigma come strato di evidenza

CertiSigma fornisce questo strato. Permette ai fornitori di trasformare file ordinari in evidenza verificabile senza caricare il contenuto sottostante. Il file resta dentro l'organizzazione del fornitore. Viene calcolato un hash crittografico, l'hash viene attestato e collegato a un manifest. Il risultato è un dossier che mostra non solo ciò che il fornitore dichiara, ma quali file esistevano, in quale versione e in quale momento.

Il principio è semplice: prova fuori, contenuto dentro, contesto sotto controllo dell'organizzazione.

CertiSigma non è una certificazione NIS2, un parere legale o un sostituto del lavoro reale di sicurezza. Non valuta il contenuto del dossier, non verifica la qualità delle misure dichiarate, non controlla che il fornitore abbia effettivamente applicato le procedure e non sostituisce la revisione del cliente. L’attestazione rafforza esistenza, integrità e collocazione temporale degli artefatti; non trasforma gli artefatti in verità, conformità o adeguatezza. Prova qualcosa di più stretto e molto utile: che uno specifico oggetto digitale, o un manifest di oggetti digitali, esisteva in una forma specifica e può essere successivamente verificato rispetto a quella prova.

La documentazione developer di CertiSigma descrive una API di attestazione per hash SHA-256, con attestazione e verifica singola o batch. La documentazione SDK descrive un modello di prova a tre livelli: firma ECDSA immediata T0, timestamp RFC 3161 T1 tramite TSA esterna e ancoraggio Bitcoin T2 via OpenTimestamps. Census estende questo modello a scansione di directory, calcolo locale degli hash dei file, creazione di manifest, controlli di integrità e flussi di lavoro dell’evidenza.

Per l'evidenza del fornitore NIS2, questo è il ponte mancante tra lavoro operativo e fiducia del cliente.

5. Perché conta per i fornitori indiretti

I clienti soggetti a NIS2 o a requisiti analoghi di sicurezza della supply chain non chiedono solo se i controlli esistono. Chiedono evidenza. Questa evidenza può includere elenco accessi, report di backup, evidenze dei test di ripristino, snapshot firmware, inventari dispositivi, registri interventi, registri subfornitori, procedure di incidente, export di configurazione, screenshot, report di audit, lettere di risposta al cliente e manifest dei file.

Senza uno strato tecnico di evidenza, questi file restano fragili. Possono essere modificati, duplicati, smarriti, sostituiti o contestati. Il fornitore può faticare a provare quale versione esatta fosse disponibile al momento della risposta al cliente.

Con CertiSigma, il dossier diventa più robusto: ogni file può essere sottoposto a hash, ogni hash può essere attestato, il manifest può essere sigillato, il pacchetto di evidenza può essere verificato in seguito e il cliente può ricevere un dossier strutturato invece di una cartella caotica.

Questo non trasforma il fornitore in un dipartimento conformità. Lo trasforma in un partner leggibile, verificabile e commercialmente difendibile.

6. Tre modalità di adozione

Folder-Based Mode: Census

Per i piccoli fornitori, il punto di partenza più semplice è una cartella di evidenza. Il fornitore inserisce i file rilevanti in una client dossier folder. Census scansiona la directory, calcola SHA-256 hashes, salva un manifest e può attestare i file hashes. Il fornitore passa da "*i file ci sono da qualche parte*" a "*questo è il pacchetto di evidenza che abbiamo preparato, e questo è il suo manifest*".

Questa modalità è adatta a installatori, facility provider, studi professionali, manutentori, operatori logistici, non-profit, scuole e altri fornitori che hanno bisogno di un modo low-friction per inventariare e preservare cartelle di evidenza.

Workflow Mode: SDK Integration

Per fornitore più tecnici, l'SDK permette di integrare la creazione di evidenza nei flussi di lavoro esistenti. Una software house può attestare release reports. Un MSP può attestare monthly security reports. Una SaaS platform può attestare exported client pacchetti di

evidenza. Una web agency può attestare report di backup e incident records. Un OT maintainer può attestare configuration backup manifests.

Il fornitore non deve riprogettare l'azienda. Aggiunge un passaggio leggero di evidenza al flusso di lavoro.

Embedded Mode: API Integration

Per piattaforme e managed services, CertiSigma può essere embedded direttamente. Un client portal può generare un dossier e attestare il relativo manifest. Un tool GRC-lite può attestare pacchetti di evidenza caricati. Una managed service platform può attestare periodic reports. Un flusso documentale può hashare e attestare file finali. Una software pipeline può attestare releases, SBOM o provenance artefacts.

In questo modello, la generazione di evidenza diventa automatica. Il fornitore non deve ricordarsi di provare. Il sistema produce prova come parte del lavoro normale.

7. Perché è diverso dalla notarizzazione una tantum

L'evidenza del fornitore NIS2 non è un problema di notarizzazione una tantum. Non si tratta di timestampare un contratto una volta all'anno. È un problema ricorrente di ciclo di vita dell'evidenza.

Ogni dossier del fornitore cambia nel tempo. Cambiano elenco accessi, report di backup, versioni firmware, contatti per incidenti, subfornitori, log di manutenzione, release software, cloud provider e personale.

Se l'evidenza viene prezzata, gestita o percepita come un atto premium file-per-file, i fornitori non la adotteranno su scala. La proposition commerciale deve essere diversa: la prontezza dell'evidenza deve essere accessibile, ripetibile e operativamente normale.

Questo è il ruolo strategico di CertiSigma nel playbook. Non è uno strato cerimoniale di notarizzazione. È un low-friction strato di evidenza per attestazioni ricorrenti, flussi di lavoro in batch, manifests e integrazione nei processi ordinari.

8. Prova fuori, contenuto dentro

CertiSigma separa lo strato di prova pubblico dall'identità aziendale e dal contenuto dei documenti. Lo strato di prova pubblico ruota attorno a hash e cryptographic evidenza. Metadata organizzativi e business context restano sotto il controllo dell'API-key owner e non vengono esposti sui endpoint pubblici di verifica. I sensitive metadata possono essere client-side encrypted quando opportuno.

Questo è essenziale per i dossier dei fornitori. Il fornitore non dovrebbe caricare contratti, screenshot, registri, elenco accessi, report o materiale operativo sensibile solo per dimostrare che esistevano. I contenuti devono restare dentro l'organizzazione. La prova deve essere esterna, verificabile e separata da divulgazioni non necessarie.

Il messaggio è semplice: CertiSigma non chiede ai fornitori di pubblicare documenti o segreti aziendali. Crea uno strato di prova verificabile attorno agli hash, mentre contenuto, contesto e identità restano sotto controllo organizzativo.

9. Che cosa CertiSigma prova e non prova

CertiSigma rafforza lo strato di evidenza, ma non va presentato oltre i suoi limiti.

Può aiutare a provare:

- che un file esisteva in una specifica forma digitale;
- che un file corrisponde a un hash precedentemente attestato;
- che un dossier manifest identifica uno specifico insieme di file;
- che un report o pacchetto di evidenza non è cambiato senza che la modifica sia rilevabile;
- che un fornitore può ricostruire che cosa è stato inviato o preparato.

Non prova:

- che il contenuto di un documento sia vero;
- che un control sia efficace;
- che un backup ripristini davvero con successo;
- che un fornitore sia conforme a NIS2;
- che un obbligo legale sia stato adempiuto;
- che un cliente debba accettare l'evidenza senza review.

Questa distinzione è essenziale. CertiSigma non sostituisce la disciplina operativa. Preserva e rafforza l'evidenza prodotta da quella disciplina.

10. Il messaggio del fornitore

Un fornitore che usa questo quadro può dire in modo sicuro:

Non stiamo rivendicando una certificazione NIS2. Stiamo fornendo un dossier di evidenza strutturato per il servizio che vi eroghiamo. Il dossier include file rilevanti, limiti dichiarati, confini di responsabilità e un manifest. Dove applicabile, i file o il manifest sono stati crittograficamente attestati, in modo che esistenza, versione e integrità possano essere verificate successivamente.

È un messaggio sicuro, credibile e commercialmente forte. Evita overclaim, falsa conformità e rassicurazioni vaghe, e consegna al cliente qualcosa che può archiviare, riesaminare e difendere.

11. Posizionamento CertiSigma in questo playbook

Il posizionamento è diretto: questo playbook dice ai fornitori quale evidenza organizzare, CertiSigma rende quell'evidenza strutturata, accessibile e verificabile.

La promessa centrale è: CertiSigma trasforma l'evidenza del fornitore da file sparsi in fiducia tracciabile.

Un'altra formula utilizzabile: aiutiamo i fornitori indiretti a restare nella chain rendendo la loro evidenza strutturata, accessibile e verificabile.

La versione più forte e breve: Dalla fiducia verbale alla fiducia tracciabile.

Riferimenti developer per questa sezione:

https://developers.certisigma.ch/

https://developers.certisigma.ch/sdk

https://developers.certisigma.ch/census

Parte III: playbook settoriali

Tutti i dossier settoriali seguono lo stesso principio: non certificano la conformità NIS2. Documentano perimetro del servizio, evidenza, limiti, dipendenze e file verificabili del fornitore. Ogni playbook può essere usato da solo o combinato quando un fornitore ricade in più categorie.

I playbook non sono checklist normative. Sono modelli di raccolta evidenza da adattare al servizio effettivo, al rischio, al contratto e alle richieste del cliente.

Non tutte le voci si applicano a ogni fornitore. Una voce non applicabile dovrebbe essere marcata come "non applicabile" con breve motivazione, non semplicemente omessa.

Installatori di sistemi connessi

Quando si applica: Installatori, tecnici e imprese che lavorano su sistemi digitali, in rete o gestibili da remoto: videosorveglianza IP, citofonia connessa, controllo accessi, sistemi antintrusione, building automation/BMS, dispositivi IoT, manutenzione remota, app connesse al cloud e sistemi collegati alle reti del cliente.

Che cosa vede il cliente: Un dispositivo connesso non è più solo hardware. È un possibile punto di ingresso nel perimetro digitale del cliente. Il cliente vuole sapere se le password di fabbrica sono state cambiate, se le versioni del firmware sono note, se l'accesso remoto è dichiarato e controllato, se il segmento di rete è documentato e se le responsabilità di manutenzione sono chiare.

Errore comune: Pensare che "*ci pensa il prodotto*". Hardware di qualità non significa configurazione sicura. Credenziali di default, firmware privo di patch, accesso remoto permanente e non monitorato e collegamenti di rete non documentati creano rischio.

Aree chiave di evidenza

- Scheda di installazione: cliente, sito, data, tipo di sistema, dettagli di rete/cloud/accesso remoto, account amministrativi, responsabilità di manutenzione.
- Inventario dei dispositivi: tipo, modello, numero di serie, IP, versione del firmware al collaudo, modalità di connessione e stato.
- Dichiarazione di cambio delle credenziali di default: evidenza di processo, non password in chiaro.
- Istantanea del firmware al collaudo e dichiarazione sulla responsabilità degli aggiornamenti.

- Modello di accesso remoto: temporaneo o permanente, utenti autorizzati, MFA, revoca e registrazione.
- Note sull'esposizione di rete: presenza su Internet, uso di cloud/app, porte, VPN e responsabilità del firewall lato cliente.
- Checklist di collaudo cyber come integrazione al collaudo funzionale.
- Registro di manutenzione, confini di responsabilità, lacune e raccomandazioni.

Dossier consigliato: Connected Systems Installation Dossier

Checklist minima

- ☐ Scheda di installazione esistente
- ☐ Elenco dei dispositivi completo
- ☐ Versione del firmware documentata
- ☐ Password di default cambiate
- ☐ Account amministrativi elencati
- ☐ Accesso remoto dichiarato e controllato
- ☐ Segmento di rete indicato
- ☐ Checklist di collaudo usata
- ☐ Registro di manutenzione mantenuto
- ☐ Confini di responsabilità chiari
- ☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Connected Systems Installation Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: Gli installatori che consegnano sistemi documentati e governabili vengono scelti non solo per abilità tecnica, ma per trasparenza sul rischio.

MSP, consulenti IT e system integrator

Quando si applica: Provider che gestiscono Microsoft 365, Google Workspace, email, utenti, account amministrativi, MFA, backup, server, firewall, VPN, endpoint, EDR/antivirus, patching, helpdesk, accesso remoto, monitoraggio, tenant cloud, accessi privilegiati, incident response e continuità operativa.

Che cosa vede il cliente: Il cliente vede dipendenza. Si affida a te per dimostrare che MFA è attiva, i backup funzionano, i restore sono testati, le patch sono applicate, gli account

sono chiusi e gli incidenti sono comunicati. Sei una parte visibile della sua postura di rischio.

Errore comune: Rassicurare senza documentare. "*È tutto sotto controllo*" non è evidenza. Il cliente ha bisogno di report, export, logs e versioned files.

Aree chiave di evidenza

- Managed services perimeter: sistemi inclusi/esclusi, responsabilità, frequency, tools, reports e limiti.
- Admin elenco accessi: users, platforms, privileges, MFA status, date di creation/revision e revocation process.
- MFA status: covered systems, accounts, exceptions e verification date.
- Accesso remoto tools: software, authorised users, authentication, MFA, registrazione delle sessioni e revocation.
- Report di backup: ambito, frequency, retention, alerts, encryption, exclusions e restore tests.
- Patch report: period, systems updated, pending items, exclusions e next actions.
- Endpoint/security report: protected/unprotected dispositivi, agent status, alerts e anomalies.
- Incident communication procedure e intervention log.
- Subfornitore register e periodic monthly/quarterly reports.

Dossier consigliato: MSP Client Dossier

Checklist minima

☐ Managed services list chiara
☐ Admin access documentato
☐ MFA verificata ed exceptions annotate
☐ Accesso remoto dichiarato e controllato
☐ Report di backup aggiornato
☐ Restore test documentato
☐ Patch report disponibile
☐ Endpoint report disponibile
☐ Incident procedure definita
☐ Intervention log mantenuto
☐ Subfornitori elencati
☐ Limiti contrattuali dichiarati

☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro MSP Client Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: Gli MSP che confezionano operational visibility diventano indispensabili. Smettono di vendere ore e iniziano a vendere documented security operations.

Software house, SaaS provider e agenzie web tecniche

Quando si applica: Custom software, SaaS B2B, web app, portali, e-commerce, mobile app, booking platforms, CRM, internal tools, hosting, maintenance, API integrations, automations, plugins, siti critici e piattaforme che gestiscono login utente o dati del cliente.

Che cosa vede il cliente: Il cliente vede una dipendenza digitale. Chiede chi accede a codice e produzione, come sono gestite le release, se test e produzione sono separati, se backup e restore sono documentati, come vengono tracciate dipendenze e vulnerabilities, dove sono conservati i secrets e chi sono i cloud subfornitori.

Errore comune: Dire “usiamo GitHub”. Un repository non è governance. Controllo degli accessi, code review, gestione delle release, separazione degli ambienti, monitoraggio delle dipendenze e gestione dei segreti devono essere dimostrati.

Aree chiave di evidenza

- Service architecture: components, database, hosting/cloud, environments, integrations, APIs, authentication, roles, backups, logs e subfornitori.
- Repository access: platform, users, roles, admins, developers, collaborators, service accounts, MFA, access review dates e revocation.
- Code review process: policy, pull requests, branch rules e approvals.
- Release management: version, date, content, bug fixes, security updates, downtime, approver e rollback plan.
- Environment separation: development, test, staging e production, data used, access rules e deployment method.
- Backup: code e database, frequency, retention, location, encryption, access, restore procedure e last test.
- Dependency and vulnerability management.
- Secrets e API key management senza esporre secrets.

- Accesso alla produzione, log applicativi, registro dei cloud provider e log di change/manutenzione.
- Incident communication procedure.

Dossier consigliato: Digital Service Security Dossier

Checklist minima

- ☐ Service sheet completa
- ☐ Architecture documentata
- ☐ Data ambito chiaro
- ☐ Repository access elencato
- ☐ Code review process definito
- ☐ Release register mantenuto
- ☐ Environments separati
- ☐ Production controllo degli accessilato e MFA abilitata dove applicabile
- ☐ Secrets gestiti in sicurezza
- ☐ Database backup e restore testati
- ☐ Dependencies monitorate
- ☐ Vulnerabilities tracciate
- ☐ Logs descritti
- ☐ Cloud subfornitori elencati
- ☐ Incident procedure definita
- ☐ Change log mantenuto
- ☐ Responsibility limiti dichiarati
- ☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Digital Service Security Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I software provider che dimostrano governance vincono contratti non solo su speed o price, ma su operational maturity e defensible delivery.

Manutentori tecnici, OT e macchinari industriali

Quando si applica: Tecnici che assistono macchine industriali, linee produttive, PLC, HMI, SCADA, reti OT, pannelli di automazione, robotica, controllo di processo,

teleassistenza, aggiornamenti firmware/software, backup delle configurazioni, sistemi di monitoraggio, attuatori, sensori e impianti che incidono sulla continuità produttiva.

Che cosa vede il cliente: Il cliente vede dipendenza operativa. Chiede quali sistemi tocchi, come funziona l'accesso remoto, come vengono autorizzati gli interventi, se le configurazioni sono backed up, se la separazione IT/OT è nota, chi contattare in emergenza e che cosa succede in caso di production stop.

Errore comune: Entrare, sistemare, uscire. Efficace nel breve periodo, fragile nel lungo. Interventi non registrati, accesso remoto permanente, configuration backups mancanti e confini IT/OT non definite creano unmanaged risk.

Aree chiave di evidenza

- Systems touched list: cliente, sito, macchina/linea, PLC/HMI/supervisor, software, network segment, access mode, criticità, contract e contacts.
- Accesso remoto model: tool, permanent vs temporary, users, MFA, authorisation, registrazione, revocation e manufacturer access.
- Intervention authorisation: ticket, email o ordine, requester, technician, system, purpose, outcome e modifications.
- Maintenance log: date, site, machine, technician, activity, configuration changes, files saved, updates, downtime e recommendations.
- Configuration backups: pre/post intervention, versioning, machine linkage, storage location, copies, protection e restore capability.
- Descrizione della separazione IT/OT e limiti noti.
- Minimum production stop plan ed contatti di emergenza.
- Update strategy e rischio operativos/recommendations.

Dossier consigliato: OT & Technical Maintenance Dossier

Checklist minima

- ☐ Systems list esistente
- ☐ Ambito chiaro
- ☐ PLC/HMI/supervisors elencati
- ☐ Accesso remoto dichiarato e controllato
- ☐ Accesso remoto autorizzato
- ☐ Interventi autorizzati
- ☐ Registro di manutenzione mantenuto
- ☐ Configurations backed up prima delle modifiche
- ☐ Backups datati e collegati

☐ Storage location nota

☐ Relazione IT/OT descritta

☐ Limiti di network segmentation annotati

☐ Production stop plan esistente

☐ Emergency contacts aggiornati

☐ Updates pianificati/documentati

☐ Operational risks e recommendations annotati

☐ Confini di responsabilità chiari

☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro OT & Technical Maintenance Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I tecnici che lasciano interventi traceable, recoverable e bounded diventano indispensabili negli ambienti produttivi regolati.

Studi professionali e document management provider

Quando si applica: Studi legali, consulenti fiscali e contabili, HR/payroll provider, consulenti tecnici, consulenti amministrativi, document management provider, servizi di archiviazione e imprese che gestiscono contratti, fatture, dichiarazioni fiscali, legal files, technical reports, PEC/email, cloud drive e shared portals.

Che cosa vede il cliente: Il cliente vede custodi di informazioni critiche. Chiede quali dati tratti, dove sono archiviati, chi vi accede, quali software/cloud provider sono coinvolti, come vengono condivisi i file, quali regole di backup e recovery si applicano e come sono gestiti incidenti o documenti inviati per errore.

Errore comune: Pensare che “sono solo documenti”. I documenti spesso contengono dati personali, finanziari, legali o strategici. Sharing non controllato, account condivisi, backup mancanti e incident response non definita creano rischio di supply chain.

Aree chiave di evidenza

- Service sheet: client, service type, document categories, channels, software, contacts, limiti e period.
- Data categories handled: personal, financial, payroll, legal, technical, administrative, PEC e official communications.
- Software and archives used: accounting, HR, document management, cloud, PEC, e-signature e portals.

- Controllo degli accessi: users, roles, privileges, MFA, revision dates, revocation e departing staff.
- Document sharing rules: allowed/prohibited channels, email vs PEC vs portal, link restrictions ed error handling.
- Email/PEC management: authorised users, access mode, MFA, archiving, attachment handling e compromise/misdirection procedure.
- Backup and recovery, staff confidentiality e software/provider register.
- Incident procedure e responsibility limiti.

Dossier consigliato: Professional & Document Management Dossier

Checklist minima

- ☐ Service sheet completa
- ☐ Data categories identificate
- ☐ Software/archives elencati
- ☐ Accessi documentati e ruoli definiti
- ☐ Accessi ex-staff revocati
- ☐ Sharing rules definite
- ☐ Email/PEC controllo degli accessilato
- ☐ MFA attiva dove disponibile
- ☐ Backup esistente e recovery testata dove possibile
- ☐ Regole di staff confidentiality presenti
- ☐ Software providers mappati
- ☐ Incident procedure definita
- ☐ Responsibility limiti dichiarati
- ☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Professional & Document Management Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: Gli studi professionali che dimostrano document governance mantengono i clienti non solo per competenza, ma per operational reliability e risk transparency.

Logistica, magazzino e trasporti

Quando si applica: Operatori che gestiscono shipments, warehousing, fulfilment, tracking, WMS/TMS, courier platforms, order/reservation management, e-commerce/ERP data flows, prova of delivery, inventory e returns.

Che cosa vede il cliente: Il cliente vede una dipendenza di continuità operativa. Chiede quali sistemi supportano il servizio, chi accede a ordini e dati, se backup ed export sono disponibili, che cosa succede se WMS o tracking non funzionano, chi sono i subfornitori critici, se esistono procedure manuali di fallback e come vengono registrati gli incidenti.

Errore comune: Pensare che il rischio sia solo fisico. Digital disruption come downtime WMS, tracking outage, shipment data corrotti, account compromessi o API integrations rotte diventano immediatamente paralisi operativa.

Aree chiave di evidenza

- Logistics systems list: WMS, TMS, tracking portal, label/picking/scanning systems, courier portals, ERP/e-commerce integrations, API/file flows, return platforms, customer service logistics, reporting, prova of delivery e inventory systems.
- System details per platform: provider, data handled, users, criticità, fallback, backup/export, support contact e dipendenze.
- User controllo degli accessi: active users, roles, client users, courier/partner users, account condivisi, MFA, review dates e revocation.
- Logistics data backup: covered data, frequency, retention, responsible party, recovery mode, uncovered data e third-party dipendenze.
- Transport and platform subfornitori.
- Procedure manuali di fallback.
- Incident register ed contatti di emergenza.
- Data handling, tracking availability, WMS details e client integrations.

Dossier consigliato: Logistics Continuity Dossier

Checklist minima

☐ Service sheet esistente

☐ Critical systems elencati

☐ WMS/tracking identificati

☐ Dati del cliente flows descritti

☐ Integrations/API annotate

☐ Accessi documentati e ruoli definiti

☐ Shared accounts limitati o dichiarati
☐ Logistics data categories annotate
☐ Backup/export esistente
☐ Backup/recovery responsibility chiara
☐ Couriers/platforms/subfornitori elencati
☐ WMS fallback esistente
☐ Tracking fallback esistente
☐ Incident register mantenuto
☐ Emergency contacts definiti
☐ Client notification process chiaro
☐ Service limiti/responsibilities dichiarati
☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Logistics Continuity Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I provider logistici che mappano le digital dipendenze, dichiarano fallbacks e tracciano incidenti diventano partner preferiti nelle supply chain regolate.

Facility management e building services

Quando si applica: Facility manager, property manager, manutentori di edifici, BMS operators, controllo degli accessi manager, CCTV/intercom provider, climate/automation maintainers, sensor/network technicians, reception/access managers e amministratori di edifici corporate o operativi con sistemi digitali.

Che cosa vede il cliente: Il cliente vede una physical-dipendenza digitale. Chiede chi controlla badge e sistemi di controllo accessi, chi vede le filmati CCTV, come viene gestito l'accesso remoto, se il BMS è documentato, come sono organizzate le reti tecniche, che cosa succede se controllo degli accessi, CCTV o BMS falliscono e come vengono registrati gli incidenti.

Errore comune: Trattare i sistemi digitali dell'edificio come infrastruttura puramente fisica. Controllo degli accessi, CCTV, BMS, sensor networks e maintenance portals hanno utenti, credenziali, firmware, logs, cloud links e responsabilità.

Aree chiave di evidenza

- Building systems list: controllo degli accessi, badges, turnstiles, electronic locks, CCTV, intercom, intrusion, BMS, climate/automation, sensors, connected elevators, connected fire systems, reti tecniche, maintenance portals, ticketing e visitor management.
- Technical provider register: name, service, systems/areas, physical/digital/accesso remoto, data handled, criticità, contact, ambito e responsibilities.
- Controllo degli accessi documentation: controlled areas, roles, admin users, badge creation/revocation, visitor/contractor management, logs, retention e failure mode.
- CCTV documentation: systems, covered areas, authorised viewers/exporters, retention, maintenance, accesso remoto e network.
- BMS/automation documentation, technical network description, maintenance log e incident register.
- Client-provider responsibility matrix, piano di continuità dell'edificio, contatti di emergenza, lacune e raccomandazioni.

Dossier consigliato: Building & Technical Services Dossier

Checklist minima

- ☐ Building/ambito sheet esistente
- ☐ Digital systems elencati
- ☐ Technical providers identificati
- ☐ Physical/digital access annotato
- ☐ Controllo degli accessi administration documentata
- ☐ Badge creation/revocation procedure esistente
- ☐ Visitors/contractors gestiti
- ☐ CCTV access/retention documentati
- ☐ BMS descritto e mantenuto
- ☐ Technical networks mappate o limiti dichiarati
- ☐ Registro di manutenzione mantenuto
- ☐ Access/system incidents registrati
- ☐ Responsabilità client-provider chiare
- ☐ Continuity plan esistente
- ☐ Emergency contacts aggiornati
- ☐ Gaps e recommendations annotati
- ☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Building & Technical Services Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I facility provider che trattano gli edifici come infrastruttura digital-physical documentata diventano indispensabili per continuità e conformità.

Sanità, assistenza e servizi alla persona

Quando si applica: Studi medici, cliniche, laboratori, centri diagnostici, home care provider, healthcare platforms, telemedicine services, centri di fisioterapia/infermieristica, booking provider, fornitori di medical device digitali, società di report management e piattaforme cliniche/agenda.

Che cosa vede il cliente: Il cliente vede un doppio rischio: protezione dei dati sanitari, personali e clinici, e continuità del servizio se i sistemi di cura falliscono, i report non sono disponibili, le piattaforme sono offline o i device non sono accessibili.

Errore comune: Confondere documentazione privacy e sicurezza operativa. Consensi e policy sono necessari, ma insufficienti. Il cliente ha bisogno anche di accessi controllati, dispositivi gestiti, condivisione sicura, backup testati, risposta agli incidenti, fornitori software noti e procedure minime di continuità.

Aree chiave di evidenza

- Health data list: identifiers, contact data, health data, diagnoses, reports, exams, images, therapies, prescriptions, care plans, patient records, operator data, caregiver/family data, billing data e device/app-collected data.
- Authorised access and roles: physicians, nurses, care operators, therapists, technicians, admin, coordinators, labs, reception, caregivers, technical providers e system admins.
- Documentazione piattaforma/registro: provider, funzione, dati trattati, utenti, ruoli, amministratori, MFA, backup, export, supporto, continuità, log e procedura di indisponibilità.
- Device usage rules: authorised dispositivi, personal vs corporate, screen lock, encryption, updates, local storage, loss/theft e technical support.
- Report/document sharing rules.
- Data/service incident register.
- Procedura di continuità assistenziale e contatti di emergenza.
- Software/provider register e responsibility limiti.

Dossier consigliato: Healthcare & Care Services Dossier

Checklist minima

- ☐ Service sheet esistente
- ☐ Health data categories identificate
- ☐ Reports/records/plans gestiti
- ☐ Roles definiti
- ☐ Accessi documentati per role
- ☐ Platform access elencato
- ☐ Accessi ex-staff revocati
- ☐ MFA attiva dove applicabile
- ☐ Platforms elencate
- ☐ Software/cloud providers identificati
- ☐ Devices elencati e rules definite
- ☐ Mobile/off-site rules presenti
- ☐ Sharing channels definiti e secured
- ☐ Error/incident procedure esistente
- ☐ Incident register mantenuto
- ☐ Platform failure procedure esistente
- ☐ Continuità assistenziale minima definita
- ☐ Emergency contacts aggiornati
- ☐ Responsibility limiti chiari
- ☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Healthcare & Care Services Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I provider sanitari e assistenziali che dimostrano data protection e continuità del servizio mantengono fiducia nelle partnership regolate.

Retail, e-commerce e servizi digitali B2B

Quando si applica: Online retailer, e-commerce manager per clienti, web agency che gestiscono shop/hosting/maintenance, marketplace operators, CRM manager, newsletter/marketing automation provider, B2B portals, POS providers, consulenti di

payment configuration, plugin/integration manager e imprese che trattano dati del cliente, orders, payments, coupons, accounts, returns e shipping.

Che cosa vede il cliente: Il cliente vede una dipendenza commerciale-operativa. Chiede quale piattaforma regge il servizio, chi detiene admin access, come vengono gestiti i plugins, qual è lo stato di backup/restore, chi gestisce hosting/DNS/SSL, come sono trattati CRM/newsletter/data, quale incident response esiste se il sito viene compromesso e quale fallback c'è se checkout o B2B portal falliscono.

Errore comune: Dire che “è solo un sito” o “è solo uno shop”. Le piattaforme e-commerce gestiscono dati personali, ordini, pagamenti, liste marketing, integrazioni e dipendenze commerciali. Compromissione, configurazione errata o downtime colpiscono direttamente ricavi, reputazione e continuità.

Aree chiave di evidenza

- Platform sheet: technology, admin, hosting, maintenance, data handled, admin accounts, plugins/extensions, integrations, backup, payment provider, logistics links, dipendenze, support contacts e service limiti.
- Client and order data: identifiers, shipping/billing addresses, orders, products, returns, complaints, discounts, loyalty data, marketing segments, B2B data e payment references/tokens.
- Payment provider: provider, function, admin accounts, authorised roles, MFA, integration, refunds, disputes, API/plugins, responsibilities e alternatives.
- Shop/CRM admin access register.
- Plugins/extensions register.
- Hosting/domain/web agency responsibilities.
- Site and order backup.
- CRM/newsletter governance.
- Marketplace dipendenze.
- Procedura di compromissione del sito e piano di continuità operativa.
- Third-party provider list, lacune e raccomandazioni.

Dossier consigliato: E-commerce & Retail Digital Dossier

Checklist minima

- ☐ Service sheet esistente
- ☐ Platform identificata
- ☐ Hosting/DNS/SSL responsibility chiara
- ☐ Client/order data elencati

☐ Data storage location chiara
☐ Payment provider identificato
☐ Shop/CRM admin accounts documentati
☐ MFA attiva dove applicabile
☐ Ex-staff/vendor access revocati
☐ Plugin/extension list esistente
☐ Plugin update responsibility chiara
☐ Newsletter/CRM/analytics providers elencati
☐ Marketplaces e accounts annotati
☐ Site backup esistente
☐ Order backup/export esistente
☐ Restore/test documentato
☐ Compromise procedure esistente
☐ Fallback per checkout/shop/B2B definito
☐ Third parties elencate
☐ Gaps e recommendations annotati
☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro E-commerce & Retail Digital Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I digital retail provider che dimostrano platform governance, controllo degli accessi e pianificazione della continuità diventano partner commerciali affidabili.

Scuole, formazione e istituzioni educative

Quando si applica: Scuole private, training center, corporate academy, centri corsi, scuole di lingue, e-learning platforms, LMS provider, digital school services, enti di formazione finanziati, vocational training provider, centri educativi e imprese che gestiscono iscrizioni, presenze, certificati, credenziali e piattaforme didattiche.

Che cosa vede il cliente: Il cliente o ente gestore vede una educational dipendenza digitale. Chiede quali dati di studenti, famiglie e staff sono trattati, se gli account sono nominativi, se gli account condivisi sono controllati, come vengono gestiti i dispositivi, quali cloud provider sono coinvolti, che stato di backup/export esiste, come sono gestiti account compromessi e quale fallback c'è se registry o LMS falliscono.

Errore comune: Pensare che “ci pensa la piattaforma”. Le piattaforme professionali possono essere configurate in modo errato. Registri e LMS contengono dati personali, voti, comunicazioni e identità. Account non gestiti, credenziali condivise, cartelle cloud non controllate e procedure di fallback mancanti creano rischio.

Aree chiave di evidenza

- Data categories: student, family, teacher, staff, enrolment, attendance, grades, evaluations, tests, homework, disciplinary notes, communications, uploads, certificates, payments, credentials, access logs, activity tracking, images/video e special educational needs data se applicabile.
- Registry/LMS documentation: provider, function, data handled, users, roles, admins, MFA, backup, export, support, continuità operativa, logs e procedura di indisponibilità.
- Student/teacher account management: creation, approval, roles, admin rights, MFA, revocation, end-of-year/course handling, temporary accounts e account condivisi.
- Shared device rules: labs, tablets, notebooks, classroom stations, printers e loaned dispositivi.
- Cloud/educational provider register.
- Backup and export rules.
- Compromised account procedure.
- Staff guidance e management dossier.
- Continuità educativa e limiti di responsabilità.

Dossier consigliato: Educational Services Dossier

Checklist minima

- ☐ Service sheet esistente
- ☐ Data categories identificate
- ☐ Student/family/staff data inclusi
- ☐ Registry identificato
- ☐ LMS/platform identificata
- ☐ Student accounts documentati
- ☐ Teacher accounts documentati
- ☐ Account creation/revocation rules esistenti
- ☐ Shared accounts evitati o dichiarati
- ☐ MFA attiva dove applicabile

☐ Shared dispositivi elencati
☐ Lab/device rules esistenti
☐ Cloud/educational providers elencati
☐ Platform data handling chiaro
☐ Backup/export procedure esistente
☐ Dipendenza dal provider chiara
☐ Compromised account procedure esistente
☐ Incident register mantenuto
☐ Staff istruito
☐ Registry/LMS fallback esistente
☐ Sintesi per il management esistente
☐ Responsibility limiti chiari
☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Educational Services Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: Gli educational provider che dimostrano platform governance, account management e pianificazione della continuità guadagnano fiducia da partner istituzionali e clienti corporate.

Associazioni, fondazioni e non-profit strutturate

Quando si applica: Associazioni, fondazioni, ONG, enti del terzo settore, volunteer organisations, associazioni culturali strutturate, community foundations, grant/project managers, organizzazioni che servono beneficiari, fundraising entities e non-profit che usano CRM, newsletter, cloud, payment o partner portals.

Che cosa vede il cliente: Il cliente, partner o funder vede una mission-critical dipendenza digitale. Chiede quali dati di donatori, beneficiari, volontari e personale sono trattati, chi accede a CRM, newsletter e cloud, come vengono gestiti donazioni e pagamenti, se gli accessi dei volontari sono revocati, dove sono archiviati i documenti di progetto, che backup esiste e che cosa succede se cloud, email, CRM o piattaforme di pagamento falliscono.

Errore comune: Dire "*siamo una piccola/brava non-profit*". La mission non sostituisce la governance. Donor lists, beneficiary records, volunteer databases, project documentation e payment flows sono preziosi e sensibili.

Aree chiave di evidenza

- Data categories: donors, beneficiaries, volunteers, staff, collaborators, partners, providers, payment data, donation data, communication preferences, newsletter subscriptions, event participation, project data, reporting data, images/video/testimonials, minor data, health/social data se applicabile, contracts e funder reports.
- Cloud drive and email: platforms, administrators, shared folder creators, external link sharers, sensitive folders, project access, volunteer/collaborator management, MFA, access revocation, backup/export e personal account rules.
- CRM and newsletter governance.
- Payments and donations: channels, payment provider, crowdfunding, bank transfers, donation portals, admin accounts, transaction viewers, data exporters, refunds, reconciliation, MFA e CRM integration.
- Staff/volunteer access register.
- Project document backup.
- Relevant provider register.
- Procedura per account compromessi e piano di continuità del progetto.
- Responsibility limiti e gaps.

Dossier consigliato: Partner & Funder Dossier

Checklist minima

☐ Entity/project sheet esistente
☐ Data categories identificate
☐ Donor/beneficiary/volunteer/staff data distinti
☐ Sensitive data flagged
☐ Cloud/email elencati
☐ Official folders definite
☐ Drive/email access documentati
☐ MFA attiva dove applicabile
☐ CRM/newsletter elencati
☐ List export rights chiari
☐ Payment/donation platforms identificati
☐ Donation account access chiaro
☐ Staff/volunteer access documentati
☐ Volunteer access revocati dopo attività

☐ Project document backup/export esistente

☐ Official folder per reports/contracts/evidenza esistente

☐ Relevant providers elencati

☐ Compromised account procedure esistente

☐ Incident register mantenuto

☐ Cloud/email/CRM/donation fallback esistente

☐ Gaps e recommendations annotati

☐ Responsibility limiti chiari

☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Partner & Funder Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: Le non-profit che dimostrano ordine operativo, governance degli accessi e continuità del progetto diventano più finanziabili, idonee a partnership e difendibili in collaborazioni complesse.

Accesso fisico-operativo, eventi e system testing

Quando si applica: Società di sicurezza, reception, portierato, assistenza tecnica on-site, setup AV/eventi, catering, fotografi, videomaker, società di eventi, tecnici esterni, tester, auditor, consulenti per test di continuità, penetration tester, vulnerability assessor, manutentori occasionali, personale temporaneo, trainer, steward, hostess, supporto a eventi corporate e tester di sistemi, impianti o processi.

Che cosa vede il cliente: Il cliente vede un ingresso nel physical-digital perimeter. Chiede chi entra, perché, dove può andare, chi accompagna, se vengono assegnati temporary badges o accounts, quali dispositivi vengono collegati, quali networks vengono usati, quali regole valgono per foto/video, se i test confini sono definiti, se i report sono trattati come sensitive e se l'attività viene chiusa formalmente.

Errore comune: Sottovalutare il temporary access. "*È solo oggi*", "*è solo un evento*" o "*è solo un tecnico*" produce spesso badge non tracciati, guest accounts permanenti, device connections non monitorate, credenziali non revocate e technical reports non classificati.

Aree chiave di evidenza

- Activity sheet: surveillance, assistance, event, test, audit, maintenance o temporary support; date, location, purpose, internal reference e duration.

• Physical perimeter: sites, areas, rooms, technical rooms, archives, warehouses, event spaces e accessible zones.

• Authorised persons list: external staff, technicians, event crew, testers, auditors, security, internal references, roles, ID e company.

• Entry mode: registration, temporary badges, hours, identification, escort e after-hours access.

• Area limiti e confidentiality rules, incluse photo/video rules.

• Devices and connections: laptops, AV equipment, routers, punti di accesso, testing tools, USB drives, diagnostic instruments, audio/video systems, IoT dispositivi e authorised networks.

• Guest Wi-Fi e temporary access.

• Test/audit/intervention authorisation e rules of engagement.

• Report e materiali prodotti.

• Activity log, incidents/anomalies e closure checklist.

Dossier consigliato: Physical-Operational Access Dossier

Checklist minima

☐ Activity sheet esistente

☐ Access purpose chiaro

☐ Authorised persons elencate

☐ Internal references annotate

☐ Entry mode documentato

☐ Temporary badges nominativi

☐ Access duration definita

☐ Accessible areas definite

☐ Prohibited/restricted areas annotate

☐ Escort richiesto in sensitive areas

☐ Confidentiality rules esistenti

☐ Photo/video rules esistenti

☐ Connected dispositivi elencati

☐ Guest Wi-Fi vs internal network chiari

☐ Temporary digital access documentato

☐ Temporary accounts con end dates

☐ Test/audit rules of engagement esistenti

☐ Technical reports trattati come confidential

☐ Activity log mantenuto

☐ Incident/anomaly register esistente

☐ Closure checklist definita

☐ Badges/accounts/access revocati post-activity

☐ Manifest dei file allegato

Risposta al cliente: In allegato trovate il nostro Physical-Operational Access Dossier, che documenta il perimetro di servizio rilevante, l'evidenza disponibile, le dipendenze, i limiti e il manifest dei file. Non è una certificazione NIS2 né un audit organizzativo completo. È un pacchetto di evidenza strutturato per il perimetro che forniamo.

Opportunità: I temporary access provider che documentano entry, limiti, dispositivi, testing confini e formal closure diventano trusted perimeter partners.

Parte IV: implementazione e posizionamento

Come iniziare senza sovraccaricarsi

1. Mappa il service perimeter: che cosa tocchi davvero per questo cliente?
2. Raccogli l'evidenza esistente: log, report, configurazioni, procedure, elenchi accessi e registri di backup.
3. Colma i gap minimi: procedure sintetiche, review degli accessi, verifica dei backup e contatti per incidenti.
4. Costruisci il dossier usando il playbook settoriale e aggiungi un manifest dei file.
5. Dichiara chiaramente i limiti: che cosa fai, che cosa non fai e che cosa dipende da altri.
6. Versiona e data tutto. Usa hash o attestazioni dove appropriato.
7. Scegli il livello di maturità dell'evidenza: basic, strutturato e verificabile o managed.
8. Usa Census, SDK o API integration quando i pacchetti di evidenza ricorrenti rendono troppo fragile la gestione manuale.
9. Aggiorna periodicamente e allinea il dossier a richieste del cliente, cambi di servizio e turnover del personale.

Note regolatorie

- NIS2 si riferisce alla Direttiva (UE) 2022/2555 e si applica, tramite recepimento nazionale, alle entità essenziali e importanti nei settori coperti.
- Gli obblighi di sicurezza della supply chain richiedono alle entità regolate di affrontare il rischio legato a fornitori e service provider come parte delle misure di cybersecurity risk management.
- La proporzionalità è un principio centrale: evidenze e misure devono corrispondere a criticità del servizio, accesso, esposizione dei dati, dipendenze e impatto operativo.
- Il Regolamento di esecuzione (UE) 2024/2690 riguarda categorie specifiche di soggetti digitali e non esaurisce l'intero universo NIS2 né tutti i fornitori indiretti.
- ENISA pubblica guide tecniche e buone pratiche. Sono riferimenti utili, ma non sostituiscono l'analisi legale locale né le indicazioni dell'autorità competente.
- Il recepimento nazionale e la guidance delle autorità di settore possono variare. Per l'Italia, il recepimento è avvenuto con il Decreto Legislativo 4 settembre 2024, n. 138; gli aspetti applicativi devono essere verificati sul testo nazionale e sugli atti dell'autorità competente.

Questo quadro è una guida metodologica, non un parere legale. Per obblighi specifici di giurisdizione, settore o contratto, usare consulenti qualificati.

Nota finale

NIS2 sta ridisegnando la fiducia B2B. I fornitori che sostituiscono dichiarazioni con evidenza, opacità con struttura e memoria con documentazione non si limiteranno a sopravvivere al cambiamento regolatorio. Lo guideranno. L'obiettivo non è la perfezione. È chiarezza, proporzionalità e verificabilità.

Dalla fiducia verbale alla fiducia tracciabile. Costruisci il dossier. Parla la lingua del rischio del cliente. Stay in the chain.

https://certisigma.ch/legal/imprint