

NSI ADVISOR S.R.L.

Politica per la Sicurezza delle Informazioni

Sistema di gestione per la sicurezza delle informazioni ISO/IEC 27001:2022

Versione pubblica destinata a clienti, partner, fornitori e collaboratori. Il documento dichiara i principi con cui NSI Advisor protegge le informazioni proprie e quelle che le vengono affidate, e gli impegni che assume nei confronti di chi gliele affida.

Revisione 2.0 · data di approvazione da completare. Deriva dalla Politica per la sicurezza delle informazioni del sistema di gestione (doc. 02PSI), della quale espone i soli contenuti di carattere generale.

NSI Advisor S.r.l. · Via Carlo Cattaneo 96, 20025 Legnano (MI) · P.IVA 10913080965

Sistema di gestione per la qualità ISO 9001:2015 — BSI FS748815 · Sistema di gestione per la sicurezza delle informazioni ISO/IEC 27001:2022 — BSI IS808481

1. Scopo e ambito

NSI Advisor progetta, realizza e gestisce infrastrutture di rete e servizi di cyber security. Nell'erogare questi servizi l'azienda entra in contatto con informazioni particolarmente sensibili dei propri clienti: architetture tecnologiche, configurazioni, credenziali di accesso, dati operativi, strategie e postura di sicurezza.

Per un fornitore di servizi di sicurezza gestita la protezione delle informazioni non è un adempimento interno: è la premessa stessa del servizio. Un cliente che affida a NSI Advisor il monitoraggio della propria rete o la gestione degli accessi privilegiati sta estendendo il proprio perimetro di fiducia. Questa politica dichiara come l'azienda intende esserne all'altezza.

La politica si applica a tutte le informazioni trattate — proprie, dei clienti e di terze parti — a tutti i processi e le risorse coinvolti nella progettazione, realizzazione ed erogazione dei servizi, e a tutte le persone che operano per NSI Advisor, inclusi collaboratori e professionisti esterni.

Il documento si integra con la Politica per la Qualità e con il Codice Etico e di Sostenibilità, anch'essi pubblicati.

2. I principi

La protezione delle informazioni si fonda su sei principi, che orientano ogni misura tecnica e organizzativa adottata:

- **Riservatezza:** le informazioni sono accessibili esclusivamente a soggetti e processi autorizzati, e solo per finalità legittime;
- **Integrità:** i dati sono protetti da modifiche non autorizzate o accidentali, e ne è preservata la coerenza;
- **Disponibilità:** informazioni e servizi sono accessibili alle persone autorizzate quando servono;
- **Autenticità:** la provenienza e l'affidabilità delle informazioni sono verificabili;
- **Controllo:** la gestione dei dati avviene attraverso processi e strumenti definiti, tracciabili e sicuri;
- **Protezione dei dati personali:** i trattamenti sono gestiti nel rispetto della disciplina applicabile in materia di privacy.

3. I nostri impegni

NSI Advisor si impegna, nei confronti di clienti, fornitori e terze parti, a:

- conoscere e classificare le informazioni gestite, valutandone la criticità per applicare livelli di protezione proporzionati;
- governare identità e accessi secondo i principi di necessità, autorizzazione e minimo privilegio, con particolare rigore sugli accessi privilegiati alle infrastrutture dei clienti;
- adottare misure organizzative, fisiche e tecnologiche proporzionate ai rischi e al contesto, riesaminandole periodicamente;
- valutare con regolarità rischi, minacce, vulnerabilità e opportunità connesse alla sicurezza delle informazioni;
- proteggere le sedi e le aree in cui sono trattate informazioni o custoditi asset, consentendone l'accesso al solo personale autorizzato;
- rispettare gli obblighi legali, regolamentari e contrattuali applicabili, inclusi gli impegni di sicurezza assunti con clienti e terze parti;
- mantenere la tracciabilità delle attività rilevanti, con responsabilità e criteri definiti.

4. Eventi, incidenti e vulnerabilità

Nessun sistema di protezione elimina il rischio: la differenza la fa la capacità di accorgersi in tempo e di reagire in modo ordinato.

NSI Advisor adotta processi per rilevare, segnalare, classificare e gestire tempestivamente eventi anomali, incidenti e vulnerabilità, con l'obiettivo di contenerne l'impatto e ripristinare la normale operatività. Ogni incidente rilevante è oggetto di analisi delle cause e di verifica dell'efficacia delle azioni intraprese; le lezioni apprese alimentano il miglioramento delle misure adottate.

La segnalazione tempestiva è incoraggiata e non sanzionata: una criticità comunicata presto è un problema gestibile, una criticità taciuta diventa un incidente.

5. Continuità operativa

L'azienda promuove la continuità dei servizi, la resilienza delle infrastrutture e la capacità di ripristino, definendo i parametri di riferimento e verificandone periodicamente l'efficacia attraverso prove e riesami.

Per i servizi gestiti la continuità è un impegno verso il cliente, non solo verso sé stessi: la disponibilità del presidio operativo e la ripristinabilità dei sistemi affidati rientrano fra gli elementi che qualificano il servizio.

6. Le persone e la consapevolezza

La sicurezza non è soltanto un insieme di tecnologie: è un processo continuo fatto di competenze, attenzione e responsabilità condivisa. Per questo NSI Advisor forma e sensibilizza le persone che operano per suo conto, favorendo comportamenti responsabili e una cultura della sicurezza diffusa.

Chi lavora per NSI Advisor è tenuto a rispettare le regole di sicurezza applicabili, a proteggere le informazioni cui accede e a segnalare tempestivamente anomalie, vulnerabilità o situazioni che possano migliorare la protezione dei sistemi.

7. Fornitori e terze parti

I requisiti di sicurezza si estendono a fornitori, produttori tecnologici, operatori di connettività e professionisti esterni che trattano informazioni o accedono ai sistemi nell'ambito dei servizi erogati.

NSI Advisor valuta i requisiti di sicurezza nei rapporti con le terze parti, li formalizza negli accordi contrattuali e ne verifica il rispetto nel tempo, con attenzione proporzionata alla criticità delle informazioni e degli accessi coinvolti. Il rischio di terza parte è considerato parte integrante del rischio complessivo dell'organizzazione.

8. Conformità, verifiche e miglioramento

Il sistema di gestione per la sicurezza delle informazioni di NSI Advisor è sviluppato secondo i requisiti della norma ISO/IEC 27001:2022 ed è oggetto di certificazione da parte di un ente accreditato.

L'efficacia delle misure adottate è verificata attraverso audit interni, verifiche dell'ente di certificazione, esiti della gestione degli incidenti e riesami periodici della Direzione, che sostiene il sistema, assegna responsabilità e rende disponibili le risorse necessarie.

Il sistema è mantenuto in miglioramento continuo: le misure vengono aggiornate in funzione dell'evoluzione delle minacce, delle tecnologie, dei servizi erogati e del quadro normativo di riferimento.

9. Diffusione e riesame

La presente politica è comunicata alle persone che operano per NSI Advisor ed è resa disponibile a clienti, fornitori e terze parti attraverso il sito aziendale e i canali di comunicazione previsti.

Il documento è riesaminato periodicamente dalla Direzione e aggiornato quando l'evoluzione dell'azienda, dei servizi, delle minacce o del contesto normativo lo renda necessario.

Nota sulla versione pubblica. Questo documento espone gli indirizzi generali della politica per la sicurezza delle informazioni. Procedure operative, standard tecnici, analisi dei rischi, assegnazione dei ruoli e documentazione del sistema di gestione sono documenti interni classificati e non sono oggetto di pubblicazione.