POLITICA DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI)

Edizione del Documento

Codice documento:	POLITICA DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI)
Versione:	Prima emissione
Data della versione:	01/10/2024
Redatto da:	Dario Parodi
Approvato da:	Direzione
Classificazione documento:	Di uso esclusivo di ufficio

Sede legale e direzione generale: ITALY - VEGLIE (LE)ITALY

Altre sedi: NAPOLI - ITALY – ROMA - ITALY – MILANO - ITALY – TORINO - ITALY - ORBASSANO (TO) - FRANCE – POISSY - SERBIA – KRAGUJEVAC - BRAZIL – ORLANDIA - BRAZIL - BELO HORIZONTE - BRAZIL – GOIANA - ARGENTINA – CORDOBA - USA – WILMINGTON

Storia dei cambiamenti

Data	Versione	Redatto da	Descrizione del cambiamento
01/10/2024	1	Dario Parodi Alessandro Feltrin	Rielaborazione del documento "IMPEGNO POLITICA AUTORITA' E CAMPO DI APPLICAZIONE" Pr. 02 Rev. 05 del 30.12.2022 scorporando il contesto relativo a quanto di interesse della norma ISO 20000-1:2018

SOMMARIO

Sede legale e direzione generale: ITALY - VEGLIE (LE)ITALY

Altre sedi: NAPOLI - ITALY – ROMA - ITALY – MILANO - ITALY – TORINO - ITALY - ORBASSANO (TO) - FRANCE – POISSY - SERBIA – KRAGUJEVAC - BRAZIL – ORLANDIA - BRAZIL - BELO HORIZONTE - BRAZIL – GOIANA - ARGENTINA – CORDOBA - USA – WILMINGTON

1. SCOPO

La presente Politica per la Sicurezza delle Informazioni definisce il quadro e gli impegni di N&C S.r.l. per proteggere la riservatezza, l'integrità e la disponibilità dei propri asset informativi.

La presente politica stabilisce i principi, le misure e le responsabilità necessari per implementare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001:2022, garantendo la protezione dei sistemi, dei dati e dei servizi offerti sia alla Pubblica Amministrazione che ai clienti privati.

2. AMBITO DI APPLICAZIONE

L'ambito di applicazione è il seguente:

Progettazione, sviluppo, installazione, configurazione, consulenza, assistenza, manutenzione, gestione e conduzione di impianti di rete, telefonia, telecomunicazione, trasmissione dati, data center, infrastrutture tecnologiche ICT.

Fornitura, assistenza e manutenzione di hardware e software tramite contact center.

Progettazione, sviluppo, configurazione, distribuzione, consulenza, assistenza, manutenzione, gestione e conduzione di:

- Applicativi software
- Dispositivi e sistemi integrati multimediali per la visualizzazione, l'ascolto e la trasmissione remota dei contenuti
- Servizi di sicurezza logica (Cyber-Security) e fisica (Physical-Security).

Inoltre, la presente politica si applica a:

- Tutti i sistemi, reti, applicazioni e dati utilizzati per fornire i servizi IT.
- Tutte le sedi operative, incluse le tre sedi principali (Veglie, Orbassano e Roma) e le tre sedi minori (Milano, Bologna e Napoli).
- I due Data Center situati nelle sedi Orbassano e Roma
- Il CED della sede di Veglie.
- Tutti i dipendenti, collaboratori, fornitori e terze parti che hanno accesso alle informazioni aziendali.

3. OBIETTIVI

Gli obiettivi della presente politica sono:

- Proteggere in modo efficace gli asset informativi da accessi non autorizzati, modifiche non autorizzate o divulgazioni.
- Assicurare la continuità operativa dei servizi IT critici.
- Rispettare i requisiti normativi, contrattuali e di conformità in materia di sicurezza delle informazioni.
- Promuovere una cultura della sicurezza all'interno dell'organizzazione attraverso formazione e sensibilizzazione.

Sede legale e direzione generale: ITALY - VEGLIE (LE)ITALY

Altre sedi: NAPOLI - ITALY – ROMA - ITALY – MILANO - ITALY – TORINO - ITALY - ORBASSANO (TO) - FRANCE – POISSY - SERBIA – KRAGUJEVAC - BRAZIL – ORLANDIA - BRAZIL - BELO HORIZONTE - BRAZIL – GOIANA - ARGENTINA – CORDOBA - USA – WILMINGTON

- Integrare e coordinare le attività di monitoraggio, prevenzione, risposta agli incidenti e miglioramento continuo.

4. STRUTTURA ORGANIZZATIVA E RESPONSABILITÀ

4.1. LEADERSHIP E GOVERNANCE

- **Direzione Aziendale:** È responsabile di approvare la politica, fornire le risorse necessarie e garantire l'allineamento strategico del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) con gli obiettivi di business.
- **Responsabile del SGS/Information Security Manager:** Coordina l'implementazione e il mantenimento dell'SGSI, supervisiona la gestione dei rischi e coordina le attività di monitoraggio e risposta agli incidenti.
- **Security Operations Center (SOC) / NOC:** Seppur non in presenza di un SIEM dedicato, il nostro NOC opera 24/7 per monitorare gli eventi attraverso anche attraverso il collettore di eventi basato su SPLUNK Enterprise, garantendo una rilevazione tempestiva delle anomalie.
- **Data Center Managers/Referenti di Sede:** Responsabili della sicurezza fisica e della continuità operativa dei data center situati nelle sedi Orbassano e Roma.
- **Tutti i Dipendenti:** Devono seguire le procedure stabilite, partecipare alle sessioni di formazione e segnalare eventuali incidenti o anomalie.

4.2. RUOLI SPECIFICI

- **Responsabile della Sicurezza Cyber (Interim/Designato):** Anche in assenza di un CISO dedicato, il responsabile designato per la sicurezza Cyber coordina le attività di sicurezza, definisce le politiche operative.
- **Referente interno per la Normativa NIS2 e per la compliance –** è stato designato come punto di contatto presso l'ACN, è il referente interno le tematiche Privacy che segue coordinandosi con il DPO esterno, si occupa della revisione documentale riferita ai Sistemi di gestione tecnici (ISO20000-1, ISO22301 e ISO27001), monitora costantemente le disposizioni emanate dai vari organismi e verifica l'aderenza dei Sistemi di Gestione agli standard di riferimento
- **Team IT e Operazioni:** Implementa le misure tecniche e le procedure operative, garantendo che le configurazioni siano sicure e aggiornate.
- **Team di Incident Response:** Si attiva immediatamente in caso di incidente, seguendo il piano di risposta agli incidenti e lavorando per ristabilire la normalità.
- **DPO** – N&C si avvale dei servizi di una società esterna per la gestione della privacy. La società nominata e la Carrisi Consulting SRLS che ha provveduto a nominar eil punto di contatto , Dott.re Rosario Carrisi, presso il sito del Garante.

5. GESTIONE DEI RISCHI

L'organizzazione adotta un processo strutturato di risk assessment che include:

- **Identificazione dei rischi:** Valutazione delle minacce interne ed esterne che possono compromettere gli asset informativi.
- **Valutazione dei rischi:** Analisi della probabilità e dell'impatto dei rischi, con una classificazione che consente di prioritizzare gli interventi.
- **Trattamento dei rischi:** Implementazione di misure di mitigazione, piani di continuità operativa e strategie di risposta.
- **Monitoraggio e revisione:** Audit interni ed esterni, reportistica e riesame periodico per garantire il miglioramento continuo del sistema.

6. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

- **Protezione delle Reti e dei Sistemi:**
  - Implementazione di soluzioni firewall, WAF, IDS e IPS, sistemi di autenticazione robusta (inclusa l'autenticazione multi fattore) e segmentazione della rete per isolare i sistemi critici.
  - Utilizzo di un event collector basato su SPLUNK Enterprise, monitorato da un team che opera sotto il coordinamento del Responsabile della Sicurezza CYBER, per la raccolta e analisi degli eventi
  - Gestione di eventi su infrastruttura di rete monitorati dal NOC di Orbassano
- **Gestione degli Accessi:**
  - Controllo rigoroso degli accessi mediante politiche di "minimo privilegio", con revisione periodica dei diritti di accesso.
- **Sicurezza dei Dati:**
  - Crittografia dei dati in transito e a riposo, backup regolari e strategie di disaster recovery per i sistemi e i data center.
- **Gestione degli Incidenti:**
  - Procedure documentate per la risposta agli incidenti e il ripristino dei servizi, con un protocollo di escalation e notifiche interne ed esterne.
- **Formazione e Sensibilizzazione:**
  - Programmi di formazione periodica rivolti a tutti i dipendenti, con particolare attenzione ai team IT e a quelli operativi, per garantire una solida cultura della sicurezza.

7. MONITORAGGIO E MIGLIORAMENTO CONTINUO

Il Sistema di Gestione della Sicurezza delle Informazioni sarà costantemente monitorato attraverso:

- **Key Performance Indicators (KPI):** Misurazione dei tempi di risposta agli incidenti, del numero di incidenti, dei risultati degli audit e della conformità agli standard.

- **Audit e Revisione:** Audit interni e esterni regolari per verificare l'implementazione efficace delle misure di sicurezza e individuare eventuali non conformità.
- **Management Reviews:** Riunioni periodiche per valutare l'efficacia dell'SGSI e aggiornare piani e strategie in base alle evoluzioni delle minacce.
- **Feedback e Formazione Continua:** Raccolta di feedback da parte degli utenti e del personale per identificare aree di miglioramento e aggiornare la formazione.

8. COMUNICAZIONE E REPORTISTICA

- **La Politica dell'SGSI:** La politica dell'SGSI è pubblicata sul Sito Istituzionale per condividerla con tutti gli stakeholder.
- **Documenti di Sistema:** sull'Intranet aziendale sono pubblicati i documenti rilevanti per aumentare la consapevolezza degli stakeholder interni riguardo le politiche SGSI. Comunque, tutte le politiche, tutti i processi, le procedure e le revisioni sono documentati e conservati secondo una rigorosa politica di controllo documentale, per garantire tracciabilità e conformità.
- **Comunicazione Interna:** I risultati del monitoraggio, gli audit e gli incidenti sono comunicati tempestivamente al management e a tutte le parti interessate interne.
- **Comunicazione Esterna:** In caso di incidenti gravi, sono adottate le procedure di notifica previste, in conformità alle normative vigenti e ai requisiti dei clienti.

9. ESTENSIONI: ISO 27017 E ISO 27018

Per rafforzare ulteriormente il nostro Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e garantire elevati standard di sicurezza e protezione dei dati nel contesto dei servizi cloud, l'organizzazione adotta anche le best practice previste dalle norme **ISO/IEC 27017** e **ISO/IEC 27018**.

9.1. ISO 27017 – LINEE GUIDA PER LA SICUREZZA NEI SERVIZI CLOUD

L'ISO 27017 fornisce raccomandazioni specifiche per i controlli di sicurezza nella fornitura e nell'utilizzo di servizi cloud. In particolare, questa norma:

- **Definisce controlli aggiuntivi:** Specifici per il cloud computing, che includono la gestione degli accessi, la configurazione di sicurezza dei servizi cloud e il monitoraggio del traffico dati.
- **Promuove la responsabilità condivisa:** Evidenziando le aree di responsabilità sia del provider cloud che del cliente, facilitando la chiarezza nella gestione della sicurezza dei dati.
- **Supporta la trasparenza:** Incentivando la verifica periodica dei controlli di sicurezza implementati dai provider cloud e l'adozione di misure per mitigare i rischi specifici del cloud.

Sede legale e direzione generale: ITALY - VEGLIE (LE)ITALY
Altre sedi: NAPOLI - ITALY – ROMA - ITALY – MILANO - ITALY – TORINO - ITALY - ORBASSANO (TO) - FRANCE – POISSY - SERBIA – KRAGUJEVAC - BRAZIL – ORLANDIA - BRAZIL - BELO HORIZONTE - BRAZIL – GOIANA - ARGENTINA – CORDOBA - USA – WILMINGTON

La nostra organizzazione integra questi controlli per garantire che tutti i servizi cloud, utilizzati internamente o forniti ai clienti, siano configurati e gestiti in modo da soddisfare i requisiti di sicurezza raccomandati dalla **ISO 27017**.

9.2. ISO 27018 – PROTEZIONE DEI DATI PERSONALI NEI SERVIZI CLOUD

L'ISO 27018 si concentra sulla protezione dei dati personali nei contesti cloud, offrendo linee guida specifiche per la gestione e la protezione delle informazioni identificabili personalmente (**PII**). Questa norma:

- **Stabilisce misure di protezione dei dati:** Incluse la gestione delle autorizzazioni, la segregazione dei dati e il controllo degli accessi alle informazioni personali.
- **Definisce politiche per la privacy:** Facilitando la conformità al GDPR e ad altre normative sulla protezione dei dati, mediante il rispetto dei diritti degli interessati e la gestione di eventuali incidenti di sicurezza che coinvolgono PII.
- **Promuove la trasparenza e la responsabilità:** Attraverso una documentazione accurata delle misure di protezione adottate, garantendo che i fornitori di servizi cloud trattino i dati personali in modo responsabile.

La nostra organizzazione adotta un **Modello Organizzativo per la Protezione dei Dati (MOPD)**, fornito dal nostro DPO, e adotta il **framework ISO 27018** per garantire che la gestione dei dati personali nei servizi cloud sia conforme agli standard internazionali, aumentando così la fiducia dei clienti e degli stakeholder nella protezione delle informazioni sensibili.

9.3. INTEGRAZIONE CON IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Le estensioni ISO 27017 e ISO 27018 sono integrate all'interno del nostro SGSI, contribuendo a:

- **Migliorare la gestione dei servizi cloud:** Attraverso controlli di sicurezza specifici per ambienti cloud e pratiche operative che assicurino la segregazione e il monitoraggio del traffico dati.
- **Garantire la protezione della privacy:** Implementando misure per proteggere i dati personali e assicurare la conformità con le normative vigenti.
- **Fornire reportistica trasparente:** Sia per la sicurezza informatica sia per la protezione dei dati personali, in modo da facilitare audit interni ed esterni e rispondere ai requisiti dei clienti e delle autorità regolatorie.

9.4. OBIETTIVI SPECIFICI

Con l'integrazione delle norme ISO 27017 e ISO 27018, l'organizzazione si prefigge di:

- Rafforzare la sicurezza dei servizi cloud offerti e utilizzati internamente.
- Aumentare la trasparenza e la conformità nella gestione dei dati personali.
- Migliorare la resilienza cibernetica e la gestione dei rischi specifici del cloud.

Sede legale e direzione generale: ITALY - VEGLIE (LE)ITALY

Altre sedi: NAPOLI - ITALY – ROMA - ITALY – MILANO - ITALY – TORINO - ITALY - ORBASSANO (TO) - FRANCE – POISSY - SERBIA – KRAGUJEVAC - BRAZIL – ORLANDIA - BRAZIL - BELO HORIZONTE - BRAZIL – GOIANA - ARGENTINA – CORDOBA - USA – WILMINGTON

- Fornire ai clienti e agli stakeholder un elevato standard di protezione e rispetto della privacy.

10. REVISIONE DELLA POLITICA

Questa politica è rivista almeno una volta all'anno, o ogni volta che vi sono cambiamenti significativi nell'ambiente IT o nelle normative applicabili.

Le modifiche sono approvate dalla Direzione Aziendale e comunicate a tutto il personale.

Sede legale e direzione generale: ITALY - VEGLIE (LE)ITALY

Altre sedi: NAPOLI - ITALY – ROMA - ITALY – MILANO - ITALY – TORINO - ITALY - ORBASSANO (TO) - FRANCE – POISSY - SERBIA – KRAGUJEVAC - BRAZIL – ORLANDIA - BRAZIL - BELO HORIZONTE - BRAZIL – GOIANA - ARGENTINA – CORDOBA - USA – WILMINGTON