"POLITICA GENERALE DEL SISTEMA DI GESTIONE INTEGRATO"

(ISO 9001, ISO 27001 ed estensioni ISO 27017, ISO 27018, ISO 27035, ISO 22301, ISO 20000-1, ISO 14001, UNI PDR 125)

4	Paola Massolo	04/04/2025	Michele Zunino	04/04/2025
REV. VIGENTE	COMPILATO DA RSGI (FIRMA)	DATA COMPILAZIONE	APPROVATO DA DIR (FIRMA)	DATA APPROVAZIONE PER EMISSIONE

ELENCO DELLE REVISIONI		
REV	DATA	DESCRIZIONE DELLE REVISIONI
0	07/02/2023	Prima emissione
1	02/04/2024	Introduzione SSRM
2	16/07/2024	Implementazione SSRM
3	11/09/2024	Implementazione UNI PdR 125:2022
4	04/04/2025	Aggiornamento ISO/IEC 27001:2022

INDICE

1.0 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce la politica aziendale definita dalla Direzione di NETALIA relativamente al Sistema di Gestione Integrato: Qualità, Sicurezza delle Informazioni (e sue estensioni per la Sicurezza del Cloud), Continuità Operativa, Gestione dei Servizi, Gestione Ambientale e Gestione per la Parità di Genere.

La Politica ha carattere generale ed intende esprimere la volontà della Direzione aziendale di:

- accrescere la soddisfazione del Cliente;
- garantire la qualità, sicurezza delle informazioni, continuità operativa, gestione efficace nella fornitura dei propri prodotti e nell'erogazione dei propri servizi e tutela dell'ambiente e tutela della parità di genere;
- perseguire il miglioramento continuo di tutti i processi aziendali e servizi erogati con riguardo alle necessità e aspettative di tutte le parti interessate.

La Politica del Sistema di Gestione Integrato si applica a tutti i livelli e a tutte le attività svolte da NETALIA ed in particolare all'attività oggetto di certificazione.

La seguente politica, e le politiche aziendali derivanti da essa, viene rivista in caso di cambiamenti significativi o almeno una volta all'anno in occasione del riesame della Direzione eventualmente confermandone la validità.

Gestione della sicurezza delle informazioni nell'erogazione di servizi cloud

2.0 DOCUMENTI DI RIFERIMENTO

ISO 9001:2015 – Sistemi di gestione per la Qualità – Requisiti

ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti

ISO/IEC 27017:2015 – Codice di pratica per i controlli di sicurezza delle informazioni basati su ISO / IEC 27002 per i servizi cloud

ISO/IEC 27018:2019 – Codice di pratica per la protezione delle informazioni personali (PII) in cloud pubblici che agiscono come processori PII

ISO/IEC 27035:2023 –Tecnologia dell'informazione – Gestione degli incidenti di sicurezza informatica

ISO 22301:2019 – Sicurezza e resilienza – Sistemi di gestione per la continuità operativa – Requisiti

ISO/IEC 20000-1:2018 – Tecnologia per l'informazione – Gestione dei servizi – Parte 1: Requisiti per il sistema di gestione dei servizi

ISO 14001:2015 – Sistema di Gestione Ambientale – Requisiti e Guida per l'Uso

GDPR (Reg. UE 679/2016 e legislazione nazionale – D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i.)

UNI PdR 125:2022

Codice etico

SSRM

3.0 PRINCIPI DELLA POLITICA DEL SISTEMA DI GESTIONE INTEGRATO

3.1 MOTIVAZIONE

NETALIA percepisce la crescita aziendale come necessità per una maggiore diffusione della cultura della soddisfazione del cliente, della sicurezza delle informazioni e dell'erogazione dei propri servizi in maniera continuativa, efficiente e rispettosa dell'ambiente. A tale scopo, ha assunto un ruolo attivo e operativo nelle attività di impostazione e implementazione di:

- un Sistema di Gestione per la Qualità (SGQ) secondo la ISO 9001;
- un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) secondo la ISO/IEC 27001 e le sue estensioni 27017 - 27018, anche a supporto della protezione dei dati personali secondo il regolamento europeo GDPR;
- un Sistema di Gestione per la Continuità Operativa (SGCO) secondo la ISO 22301,
- un Sistema di Gestione dei Servizi (SGS) secondo la ISO/IEC 20000-1,
- un Sistema di Gestione Ambientale (SGA) secondo la ISO 14001
- un Sistema di Gestione per la Parità di genere secondo la UNI PdR 125.

Data la natura delle proprie attività, NETALIA considera, relativamente alla "Gestione della sicurezza delle informazioni nell'erogazione di servizi cloud", la qualità e la sicurezza delle informazioni fattori irrinunciabili per il miglioramento continuo delle prestazioni rese al Cliente, nell'ottica della sua soddisfazione e per la protezione del proprio patrimonio informativo, con l'obiettivo di aumentare la propria competitività sul mercato attraverso l'ottimizzazione dei propri processi progettuali, produttivi ed organizzativi.

NETALIA pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di sviluppo e realizzazione dei propri servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.

I principi di sicurezza delle informazioni si applicano a tutte le attività di analisi, sviluppo, realizzazione e manutenzione dei prodotti e servizi, ed ai dati ad esse collegati.

Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, l'organizzazione opera secondo normative di sicurezza internazionalmente riconosciute. Per questo motivo l'Azienda adotta le misure, sia tecniche che organizzative, necessarie a garantire al meglio la riservatezza, l'integrità e la disponibilità del patrimonio informativo interno (informazioni e asset) e di quello affidatole dai propri Clienti tutelandolo e proteggendolo da tutte le minacce, interne ed esterne, intenzionali o accidentali, nell'ambito delle proprie attività.

Con l'affidamento dei dati in cloud, NETALIA ha adottato l'implementazione degli standard:

- ISO/IEC 27018 che riguarda la gestione dei dati personali in relazione alle soluzioni cloud in modalità IaaS, PaaS e SaaS. La gestione dei dati personali trattati all'interno dei nostri servizi cloud è soggetta a valutazione di parte terza nei suoi aspetti tecnici, organizzativi e contrattuali;
- ISO/IEC 27017 che definisce controlli di sicurezza supplementari e rinforzati per indirizzare le misure di sicurezza messe in atto dai provider di servizi Cloud. Si attesta quindi, con valutazione di parte terza, che tali controlli sono stati integrati all'interno del Sistema di Gestione Integrato.

L'Azienda considera come ulteriori fattori determinanti per assicurare la qualità dei servizi offerti e la protezione delle informazioni, la capacità di adottare un approccio resiliente in situazioni di crisi che garantisca la continuità dell'operatività in sicurezza e la capacità di pianificazione e controllo dei servizi offerti che garantisca il soddisfacimento delle aspettative dei Clienti in maniera efficiente; il tutto, mantenendo una costante e continua attenzione ed impegno alla protezione dell'ambiente.

L'Azienda inoltre ha introdotto Il Modello di responsabilità condivisa, che è un paradigma di sicurezza che definisce ruoli e responsabilità e garantisce trasparenza tra i clienti e il provider di servizi cloud.

La piattaforma di erogazione servizi cloud di Netalia è predisposta per l'erogazione di servizi di tipo IaaS e PaaS, ognuno con diversi livelli di responsabilità. Per il dettaglio sulle funzionalità, modalità di erogazione del servizio, e sulle caratteristiche trasversali di qualità, sicurezza, privacy e continuità operativa del servizio, si rimanda al Catalogo dei Servizi.

I clienti dovrebbero valutare attentamente i servizi che scelgono in quanto le loro responsabilità varieranno in funzione dei servizi usati, dell'integrazione di quei servizi nel loro ambiente IT e delle leggi e normative applicabili.

IaaS

Per quanto riguarda il servizio IaaS, Netalia applica i controlli di seguito indicati:

- gestione e mantenimento dell'infrastruttura (fisico e infrastruttura cloud)
- attività di patching infrastrutturale (fisico e infrastruttura cloud)
- attività di configurazione infrastrutturale (fisico e infrastruttura cloud)
- formazione dei propri dipendenti.

Le restanti componenti (e la loro gestione) sono responsabilità del Cliente, inclusa la formazione dei dipendenti del Cliente.

PaaS

Per quanto riguarda il servizio PaaS la responsabilità di Netalia in questo caso prevede, oltre alle già dette componenti del servizio IaaS, anche le componenti di:

- sistema operativo
- middleware
- runtime

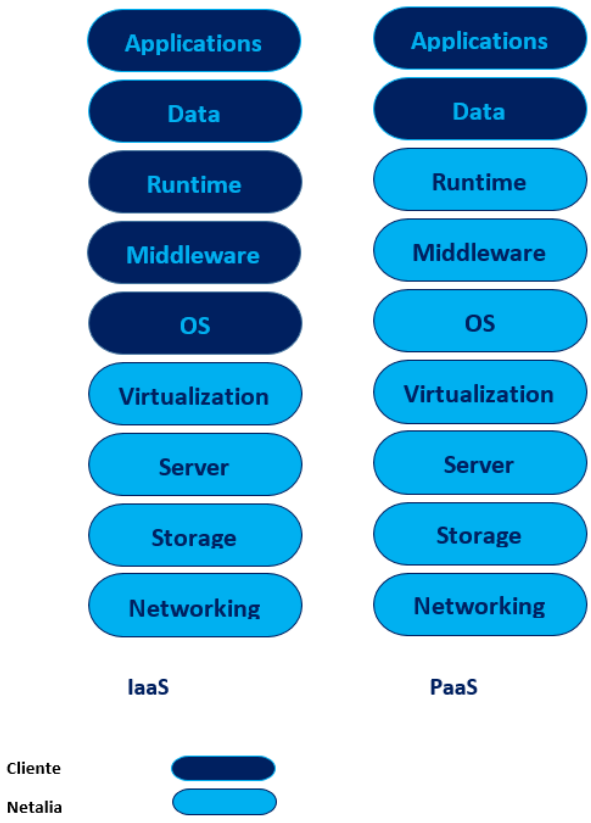
Restano di responsabilità del Cliente gli strati relativi a dati e applicazioni, nonché la loro gestione, e la formazione dei dipendenti del Cliente.

Inoltre, per tutti i tipi di servizio cloud fruito, il cliente ha la proprietà di dati e identità. L'utente del servizio cloud è responsabile della protezione dei dati e delle identità, delle risorse locali e dei componenti cloud che si controllano, che variano in base al tipo di servizio scelto.

Indipendentemente dal tipo di distribuzione, il cliente mantiene sempre le responsabilità seguenti riguardo i propri:

- endpoint
- accessi al servizio.

SSRM - Modello di responsabilità condivisa



3.2 PARITÀ DI GENERE

Netalia vuole realizzare e/o rafforzare un contesto lavorativo nel quale tutti siano ascoltati, nel quale le loro conoscenze ed esperienze vengano riconosciute, nel quale le loro aspirazioni, i loro bisogni, le loro opinioni e i loro obiettivi siano presi in considerazione e nel quale possano partecipare ai processi decisionali aziendali.

Netalia attraverso questa Politica vuole promuovere:

- selezioni ed assunzioni, gestione della carriera ed equità salariale basate sulle competenze e professionalità, prevenendo discriminazione di genere, favorendo genitorialità, cura, conciliazione dei tempi vita lavoro e adottando una Politica di tolleranza zero verso ogni forma di discriminazione.

Netalia recepito le linee guida della norma UNI/PdR125:2022 per promuovere una cultura inclusiva di accesso a mansioni aziendali e di crescita nel percorso professionale, garantendo uguali possibilità a tutto il personale e favorendo al contempo l'empowerment femminile:

- assicurando che assunzioni e promozioni a ruoli di leadership siano basate sul merito e non siano influenzate da discriminazioni di genere;
- offrendo condizioni di lavoro flessibili e congedi parentali equi per entrambi i genitori;
- garantendo parità di retribuzione, a prescindere dal genere;
- vengano definiti programmi formativi di dettaglio sulla Parità di Genere e sull'inclusione della Diversità per tutti i dipendenti interni e per tutto il personale esterno che opera per prolungati periodi all'interno dell'organizzazione qualora si verificasse quest'ultima eventualità.

A tal proposito Netalia ha nominato un Comitato Guida per l'efficace adozione e la continua applicazione di tali tematiche.

Netalia comunica il proprio impegno a tutte le parti interessate pubblicando una comunicazione "Comunicazione Parità di Genere" sul proprio sito aziendale.

Per promuovere la cultura di valorizzazione delle diversità e inclusione, la Direzione si impegna altresì a:

- nelle procedure di selezione, assicurarsi che il job profiling sia basato sui requisiti relativi al lavoro e non rifletta pregiudizi involontari, eliminare i criteri di selezione che non siano correlati al lavoro (come, ad es., il possesso di un diploma avanzato o competenze linguistiche specifiche) se non sono necessari, sviluppare strategie per ampliare il bacino di candidati, sia internamente che esternamente,

- nelle procedure di onboarding, creare processi di inserimento coerenti (in modo che tutte le persone neoassunte si sentano supportate e preparate per avere successo), concentrarsi sull'accoglienza di tutte le nuove persone e dare chiarezza su come avere successo all'interno dell'organizzazione sia attraverso processi sia formali che informali, fornire modelli di comportamento che incoraggino l'assunzione di diverse prospettive,
- nelle attività di sviluppo aziendale, incoraggiare le azioni dirette a cercare prospettive diverse per prendere decisioni e/o risolvere problemi aziendali, incorporare le pratiche D&I in tutte le attività di formazione volte allo sviluppo della leadership, delle competenze di management e delle soft skill, assicurarsi che tutti ricevano sempre feedback tempestivi in modo che sappiano come stanno lavorando, possano avere buona consapevolezza di sé e migliorare,
- nelle procedure di valutazione di performance, creare e alimentare un ambiente in cui le persone possano imparare dai propri errori, stabilire obiettivi per tutti legati alla creazione di un ambiente più inclusivo, riconoscere il miglioramento, non solo i risultati,
- assegnare risorse (budget), responsabilità ed autorità adeguate per il perseguimento, il raggiungimento ed il mantenimento degli obiettivi di parità di genere stabiliti.

Netalia ribadisce inoltre la completa adozione di principi di "tolleranza zero" rispetto ad ogni forma di violenza nei confronti dei/delle dipendenti, incluse le molestie sessuali in ogni forma.

Netalia sta attuando azioni volte ad incrementare la conciliazione vita-lavoro, nonché il principio ed obbiettivo della tolleranza zero, poi declinati nel piano strategico annuale dell'organizzazione.

3.3 OBIETTIVI

L'obiettivo del Sistema di Gestione Integrato di NETALIA è quello di garantire la sicurezza delle informazioni, la qualità, continuità ed efficienza dei servizi offerti e la tutela dell'ambiente attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali le informazioni ed i servizi stessi sono soggetti e attraverso un'adeguata comunicazione e continua formazione sulle tematiche relative al SGI che alimenti la consapevolezza, sensibilità e competenza dei propri dipendenti.

In particolare:

- nell'ambito della Qualità:
    - fornire prodotti e servizi che soddisfino i requisiti del Cliente e quelli cogenti applicabili;
    - preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;

- adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;

- nell'ambito della Sicurezza delle Informazioni:
  - proteggere al meglio il patrimonio informativo proprio e dei propri Clienti, mediante l'implementazione di opportune misure organizzative, tecniche e procedurali per:
    - salvaguardare la RISERVATEZZA delle informazioni da accessi non autorizzati, stabilendo requisiti per l'accesso e relative modalità di assegnazione dei privilegi, sia per l'accesso logico che fisico alle informazioni o agli asset aziendali;
    - assicurare l'INTEGRITÀ delle informazioni, in modo che sia modificabile solo ed esclusivamente da chi ne possiede i privilegi;
    - garantire la DISPONIBILITÀ delle informazioni agli utenti autorizzati quando ne hanno bisogno, tramite la predisposizione di sistemi di backup delle informazioni uniformemente gestiti e monitorati e la redazione di piani per la continuità dell'attività aziendale opportunamente aggiornati, controllati e migliorati;
  - assicurare la protezione dei dati personali nel rispetto dei principi e dei requisiti espressi dal GDPR, attuando misure adeguate ed efficaci che tengano conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche;
  - definire e documentare una procedura per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione, in particolar modo quando questi coinvolgano dati personali (Data Breach) con una chiara indicazione dei ruoli e delle azioni correttive da intraprendere;
- nell'ambito dell'erogazione di Servizi Cloud (Provider):
  - definire e mantenere sotto controllo:
    - le modalità di erogazione dei servizi cloud;
    - la gestione degli accessi ai servizi erogati in modalità cloud, secondo la politica di gestione degli accessi;
    - le comunicazioni ai Clienti in caso di change e agli interessati in caso di data breach;
    - il ciclo di vita degli account relativi ai servizi cloud;
    - l'esecuzione dell'analisi dei rischi derivanti dall'erogazione di un servizio cloud;

- l'applicazione dei requisiti cogenti derivati dal Regolamento Europeo per la Protezione dei Dati Personali (GDPR).

- nell'ambito della fruizione di Servizi Cloud (Customer):
  - definire e mantenere sotto controllo:
    - le modalità di conservazione e accesso alle informazioni in cloud da parte del cloud service provider;
    - se e come viene effettuato il mantenimento in ambienti multi-tenant in cloud;
    - gli utenti che fruiscono dei servizi cloud e il contesto in cui li usano;
    - gli utenti amministratori dei servizi cloud fruiti in modalità customer, dotati di accessi privilegiati;
    - la localizzazione geografica dei provider di servizi cloud e i paesi in cui il provider può conservare i dati di NETALIA, anche temporaneamente.
- nell'ambito della Continuità Operativa:
  - garantire la continuità operativa e minimizzare gli impatti sul business in situazioni di crisi, assicurando un rapido ripristino del normale stato di svolgimento delle attività aziendali;
  - definire una struttura per la risposta a scenari di crisi, in grado di gestire un'interruzione dei servizi, con una chiara definizione di ruoli e comunicazioni da eseguire;
  - pianificare e assicurare la disponibilità delle risorse sia materiali che umane, in termini di quantità e competenza, per affrontare i momenti di crisi;
  - assicurare per prima cosa la salvaguardia e la sicurezza fisica delle persone, in caso di disastro o di grave incidente;
  - migliorare la propria capacità di resilienza ad incidenti che possono determinare interruzioni delle attività critiche;
- nell'ambito della Gestione dei Servizi:
  - garantire che i propri servizi siano rispondenti agli SLA (Service Level Agreement) concordati con i rispettivi Clienti;
  - accrescere la reputazione, la credibilità e la fiducia dei Clienti nei confronti dell'Azienda che offre i propri servizi in maniera efficiente, grazie ad un approccio di standardizzazione e uniformità degli stessi ed alla relativa capacità di pianificazione e controllo.
- nell'ambito della Gestione Ambientale:

- garantire l'utilizzo delle migliori tecnologie disponibili nell'erogazione dei propri servizi riducendo al minimo l'impatto sull'ambiente.

- nell'ambito della Parità di Genere:
  - valorizzare le diversità;
  - supportare l'empowerment femminile,
  - perseguire la parità di genere, attraverso l'attribuzione di un budget annuale che permetta di raggiungere e mantenere la parità di genere,
  - mantenere comunicazioni neutre,
  - incontri periodici del Comitato Guida a supporto dell'efficacie applicazione delle politiche di parità di genere.

3.4 ANALISI DEI RISCHI

Tutte le informazioni, che vengono create o utilizzate da NETALIA, sono da salvaguardare e devono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni devono essere gestite in modo sicuro, accurato e affidabile, e devono essere prontamente disponibili per gli usi consentiti.

Con "utilizzo dell'informazione" è da intendersi qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito di applicazione, in conformità alle norme ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO 22301 e ISO 20000-1, il Responsabile per la Sicurezza delle Informazioni (CISO) svolge periodicamente un'analisi dei rischi, con lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate, che tenga in considerazione gli obiettivi strategici espressi nella presente politica, gli incidenti occorsi durante tale periodo ed i cambiamenti strategici, di business e tecnologici avvenuti.

La Direzione condivide con il Responsabile per la Sicurezza delle Informazioni (CISO) la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella redazione della metodologia la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito dell'elaborazione dell'analisi dei rischi da parte del Responsabile per la Sicurezza delle Informazioni (CISO) ed in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti considerando la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

L'analisi identifica chiaramente le azioni da intraprendere definendo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti.

L'analisi viene aggiornata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

3.5 REQUISITI

Accettazione della politica: tutti i dipendenti, collaboratori, fornitori, partner e tutte le altre parti interessate coinvolti nelle attività di NETALIA devono accettare i loro obblighi e le responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse di NETALIA o affidati a NETALIA da terzi.

Asset aziendali: NETALIA ha inventariato e mantiene costantemente aggiornato l'elenco degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno ha individuato un responsabile.

Classificazione: le informazioni gestite dall'azienda sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti ed appropriati; la classificazione risulta ad oggi di tipo Pubblica o Riservata. Ad esempio, tra i documenti del Sistema di Gestione Integrato sono presenti documenti sia pubblici (Campo di applicazione), sia riservati (le procedure).

Accesso: l'accesso alle informazioni, ai beni e alle risorse di NETALIA o affidati a NETALIA da terzi, devono essere controllati e monitorati sulla base dei seguenti criteri:

- l'accesso è autorizzato solo per le informazioni strettamente necessarie (principio di conoscenza minima);
- l'accesso è autorizzato solo per le informazioni riguardanti le specifiche attività nelle quali si è coinvolti.

Consapevolezza: la Direzione aziendale assicura che ogni dipendente, collaboratore, fornitore o parte interessata sia consapevole, attui comportamenti ed utilizzi strumenti adeguati e in linea con la presente Politica.

Formazione: la Direzione aziendale garantisce che ogni risorsa sia addestrata/formata/informata sulle politiche organizzative applicate e sulle procedure relative al SGI.

Conformità normativa e legislativa: tutti i trattamenti delle informazioni e le procedure di NETALIA sono conformi alle normative, alle leggi e ai regolamenti cogenti ed ai requisiti dei Clienti. NETALIA tutela i dati personali in accordo al vigente Regolamento Privacy REG. UE 679/2016 e D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i. e provvedimenti del Garante Privacy, al CCNL applicabile, allo Statuto dei Lavoratori, agli accordi contrattuali con i collaboratori.

Protezione: tutte le informazioni, beni e risorse di NETALIA o affidate a NETALIA da parti terze sono protette contro i rischi legati al rispetto della riservatezza, dell'integrità e della disponibilità in conformità con le leggi vigenti e in proporzione al loro valore. Le registrazioni rilevanti sono

protette da perdita, distruzione, falsificazione, accessi e divulgazione non autorizzati, in conformità con i requisiti legali, normativi, contrattuali e di business, attraverso appositi strumenti tecnici, politiche specifiche e procedure operative cui si rimanda e descritte nel SGI.

Sicurezza nella progettazione e sviluppo: NETALIA adotta un insieme di strumenti descritti nel SGI per garantire la sicurezza del processo di sviluppo, al fine di assicurare la riservatezza, l'integrità e la disponibilità delle soluzioni realizzate nell'ambito di tale processo.

Sicurezza del cloud: NETALIA consente ai clienti di definire, eseguire e sfruttare il suo ambiente di sicurezza, avendo sviluppato un programma di controlli di sicurezza che implementa best practices di protezione della privacy (ISO/IEC 27018) e dati di livello globale (ISO/IEC 27017). Queste procedure di sicurezza e controllo sono convalidate in modo indipendente tramite valutazioni di terze parti. Il programma di controlli si basa sulla verifica, la dimostrazione e il monitoraggio.

Relazioni con parti terze: NETALIA adotta la politica di responsabilizzare i propri fornitori e parti terze con cui collabora per le proprie attività, mediante specifici accordi di riservatezza e service level agreement / accordi sul livello del servizio (SLA); i suddetti accordi sono rivisti periodicamente e comunque in occasione di ogni revisione della valutazione dei rischi.

Business continuity: NETALIA predispone piani di continuità operativa ed un piano di Disaster Recovery che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale e nel rispetto dei requisiti contrattuali con i Clienti.

Tutela dell'ambiente: NETALIA valuta e presidia periodicamente i rischi e gli impatti sugli aspetti ambientali derivanti dalle proprie attività e processi, individuando ed attuando iniziative e misure per prevenire possibili incidenti con conseguenze sull'ambiente.

Riesame della politica: l'approccio di NETALIA nella gestione del SGI e della sua implementazione (requisiti, controlli, politiche, processi e procedure) viene rivisto nel periodico riesame della Direzione, o in modo indipendente dalla periodicità, quando intervengono cambiamenti significativi.

Costi: NETALIA nell'attuare quanto precedentemente definito, valuta le spese necessarie per l'attuazione delle misure al fine di: proteggere le informazioni, i beni e le risorse dall'utilizzo non autorizzato, modifiche o distruzione; assicurare la continuità dei propri servizi critici a fronte di eventi imprevisti; garantire il rispetto dell'ambiente, degli SLA e della soddisfazione del Cliente nell'erogazione dei propri servizi.

3.6 VIOLAZIONI

La violazione dei principi e dei comportamenti stabiliti nella presente Politica sarà perseguita da Netalia, nelle opportune sedi, in misura proporzionata alla gravità della violazione commessa ed in linea con i vicoli di legge e contrattuali (secondo quanto stabilito dal CCNL vigente per il personale dipendente, dalle clausole del contratto sottoscritto con i collaboratori esterni, dal REG. UE 679/2016 e D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i., dalle sentenze della giurisprudenza emesse).

4.0 RESPONSABILITÀ PER L'APPLICAZIONE DELLA POLITICA

La Direzione ha stabilito in maniera chiara e puntuale la presente Politica attraverso la definizione della propria strategia e degli obiettivi da perseguire.
La Direzione diffonde la presente Politica a tutti i livelli in modo che sia comunicata, compresa ed applicata, per ottenere l'adesione di tutti gli addetti e la loro collaborazione per il raggiungimento degli obiettivi stabiliti.

4.1 IMPEGNO DELLA DIREZIONE (DIR)

La Direzione di NETALIA ha definito, divulgato, comunicato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente Politica del Sistema di Gestione Integrato.
L'impegno della Direzione si attua tramite una struttura i cui compiti sono:

- definire ed approvare la Politica del Sistema Integrato;
- garantire che siano identificati tutti gli obiettivi relativi alla qualità, sicurezza delle informazioni, continuità operativa, gestione dei servizi e tutela dell'ambiente e che questi soddisfino i requisiti aziendali;
- raggiungere il soddisfacimento dei Clienti offrendo prodotti e servizi efficienti ed in linea con le loro esigenze;
- introdurre una maggiore flessibilità nella propria organizzazione, atta ad individuare le cause dei problemi adottando tempestivamente i provvedimenti necessari alla loro risoluzione;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGI;
- fornire risorse sufficienti e adeguate alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGI;
- controllare che il SGI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- fornire prodotti e servizi che soddisfino i requisiti del cliente, nel rispetto delle leggi, regolamenti e normative applicabili;

- privilegiare rapporti con fornitori che abbiano politiche di rispetto ambientale, accrescendo la qualità della relazione in un rapporto di reciproco beneficio;
- garantire la congruità dei budget destinati al raggiungimento degli obiettivi prefissati, coerentemente con le politiche e le linee strategiche aziendali definite;
- monitorare i cambiamenti dell'esposizione alle minacce dell'azienda, analizzare gli incidenti alla sicurezza, alla continuità ed ai servizi rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili;
- sostenere tutte le iniziative inerenti al rispetto dell'ambiente e lo sviluppo sostenibile;
- attivare programmi per la diffusione della consapevolezza e della cultura della qualità, sicurezza delle informazioni, continuità ed efficienza dei servizi erogati e tutela dell'ambiente.

4.2 IMPEGNO DEL RESPONSABILE DEL SISTEMA DI GESTIONE INTEGRATO (RSGI)

Nell'ambito del Sistema di Gestione Integrato e attraverso norme e procedure appropriate ed approvate, deve:

- effettuare l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- definire tutti i requisiti cogenti (le norme, le leggi, i regolamenti, inclusi i requisiti specifici del cliente) necessari alla gestione di tutte le attività aziendali;
- verificare le violazioni alla presente Politica e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne il Sistema Integrato;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione Integrato.

4.3 IMPEGNO DI TUTTO IL PERSONALE

Tutto il personale (dipendente e collaboratore), qualunque sia il ruolo e/o la mansione svolta, è invitato ad attuare quanto indicato:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di NETALIA o affidate a NETALIA da terze parti;
- proteggere i beni e le risorse materiali, i sistemi informatici di NETALIA o affidati a NETALIA da terze parti;
- attuare un comportamento responsabile nei confronti dell'ambiente;

- informare la Direzione ovvero il RSGI, le autorità competenti in caso di accertate e/o presunte violazioni o rilevazione di tentate violazioni;
- informare la Direzione ovvero il RSGI, in caso si ritenga necessario apportare modifiche alla presente Politica e/o ai documenti del Sistema di Gestione Integrato.

4.4 SOGGETTI ESTERNI

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda devono garantire il rispetto dei requisiti contenuti nella presente Politica.

I soggetti esterni coinvolti nel campo di applicazione del Sistema di Gestione Integrato e le linee guida di best practices sono i clienti e i fornitori, i collaboratori esterni (consulenti) operanti all'interno dell'azienda, che sono assimilabili ai dipendenti e che sottoscrivono una lettera di impegno di riservatezza.