

Dichiarazione generale di politica per la sicurezza – Ver.1.1 del 19/05/23

1 Obiettivo della politica per la sicurezza delle informazioni

La nostra organizzazione progetta e gestisce l'intera filiera IT dell'ambito *contact center* (software, risorse computazionali e connettività); la piattaforma IT denominata "NEXTIP" da noi ingegnerizzata, offre un servizio informatico, principalmente in modalità ASP (*Application Service Provider*), alle società di Contact Center, alle aziende operanti come BPO (*Business Process Outsourcer*) o alle divisioni di Contact Center / Customer Care di aziende operanti in vari settori (*finance, telco, utility*).

2 Politica appropriata alle finalità dell'organizzazione

Consapevoli che i dati del cliente, costituiscono informazioni il cui valore rappresenta il patrimonio aziendale della nostra organizzazione e di quella del cliente, abbiamo implementato un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) prevedendo la messa a punto di tutti i controlli di sicurezza applicabili al trattamento delle informazioni nei processi delle infrastrutture ICT per l'erogazione dei servizi.

Il **campo di applicazione** del nostro SGSI è allineato alle finalità della nostra organizzazione: "**GESTIONE delle INFRASTRUTTURE IT per servizi di CONTACT CENTER**"; le attività produttive inerenti al campo di applicazione sono: *l'Analisi dei Requisiti, la Progettazione e Collaudo, la Manutenzione e Assistenza Post-Vendita*.

La **sede aziendale** oggetto del nostro SGSI è l'attuale sede operativa di Via L.B.Alberti 10, in Milano.

3 Politica per fissare gli obiettivi di sicurezza

Grazie all'implementazione dell'SGSI, abbiamo determinato gli obiettivi di sicurezza delle informazioni che ci vedranno impegnati, nei processi per l'erogazione dei nostri servizi, alla preservazione della:

- **riservatezza** dei dati rilasciati dal cliente;
- **integrità** delle informazioni rilasciate dal cliente e quelle relative alle procedure di trattamento dei dati che impieghiamo per effettuare l'erogazione dei nostri servizi;
- **disponibilità** di tali informazioni alle persone autorizzate alla loro gestione e al loro impiego;
- **rispetto** delle norme cogenti in materia di trattamento dei dati personali (GDPR - D.Lgs 101/18);
- **rispetto** degli obblighi a cui nel tempo l'azienda decide di aderire.

4 Politica per l'impegno al rispetto dei requisiti applicabili

L'impegno dell'alta direzione e di tutti coloro che a vario titolo sono coinvolti dalle attività del sistema di gestione è quello di rispettare tutti i requisiti previsti dalla Norma Internazionale ISO 27001:2017. Per questo, l'alta direzione assume l'impegno di esercitare la leadership secondo quanto stabilito da tale Norma, vale a dire la valutazione di eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business o delle tecnologie utilizzate con necessità di formazione di nuove competenze o consolidamento di quelle già presenti nella nostra organizzazione;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

5 Politica per l'impegno per il miglioramento continuo del sistema di gestione

Il patrimonio informativo del cliente e quello relativo al *know-how* della nostra organizzazione costituiranno d'ora innanzi i punti focali dell'impegno di tutti. Un impegno assunto da tutti e da ciascuno.

Tale impegno sarà manifestato attraverso le "performance di sicurezza" (periodici Audit Interni, Audit con terze parti esterne anche per il mantenimento della certificazione, periodici ri-esami di direzione) che dovranno dare evidenza di quanto la nostra organizzazione ed il nostro sistema di gestione della sicurezza delle informazioni siano efficaci nel registrare un miglioramento continuo.

Ver.1.1 del 19/05/2023

Firma RGSi	
------------	--

Firma Alta Direzione	
----------------------	--