SGIG
Sistema Gestione Integrato

Politiche per il SGIG

Redazione	Verifica	Approvazione	
Aurora Maragni *Infordata S.p.A.*	**Silvia Trobbiani** *Technis Blu S.r.l.*		**Gianni Caparelli**
			Gian Luca Cafolla
			Lucia Masullo
			Gian Luca Cafolla

Registro delle modifiche

Versione	***Descrizione Modifica***	***Data***
1.0	Prima emissione	11/02/2019
1.1	Estensione politiche Cloud Infordata e introduzione al SGRS con rif. 3.7	18/05/2020
1.2	Aggiunti obiettivi per i servizi Cloud in ottica SGQ e SGS	29/06/2020
1.3	Inserimento Infordata Education	14/07/2020
1.4	Inserimento di nuovi obiettivi per il gruppo Infordata	06/07/2021
1.5	Aggiornamento per adeguamento alla ISO 45001:2018	15/04/2022
1.6	Aggiornamento per integrazione Politica per la Parità di Genere Aggiornamento par. 4.9 per predisposizione matrice sostituibilità	29/11/2022

Versione	*Descrizione Modifica*	*Data*
1.7	Aggiornamento paragrafo relativo alla politica per la sicurezza delle informazioni nelle relazioni con i fornitori	22/02/2023
1.8	Aggiornamento par. 4.8 – Politica per la Parità di Genere	19/06/2023
1.9	Aggiornamento par. 4.2.1 – per estensione delle ISO/IEC 27017 e ISO/IEC 27018 rispetto alla realtà aziendale di Eurolink S.r.l.	10/07/2023
2.0	Aggiornamento par. 4.8 – Politica per la Parità di Genere in tema di formazione integrativa a seguito di rientro dalla maternità - paternità	12/10/2023
2.1	Aggiornamento par. 4.2 per adeguamento alla nuova ISO/IEC 27001:2022	23/10/2023

Documenti di riferimento

RIF.	*Nome*
[1]	Annex SL – Proposal for management system standards (MSS)
[2]	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[3]	ISO 31000:2018 Risk Management - Guidelines
[4]	UNI EN ISO 9001:2015 – Sistemi di gestione per la qualità – Requisiti
[5]	UNI CEI ISO/IEC 20000-1:2020 Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio
[6]	UNI EN ISO 14001:2015 Sistemi di Gestione Ambientale – Requisiti e guida per l'uso
[7]	Regolamento (UE) 27/04/2016, n. 679 e Decreto Legislativo n. 196 del 30/06/2003, così come novellato dal Dlgs. 101 del 10 agosto 2018
[8]	ISO/IEC 27018:2019- Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
[9]	ISO/IEC 27017:2015- Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[10]	SA8000:2014 - Social Accountability Management Systems - Requirements
[11]	UNI EN ISO 22301:2019 – Sicurezza e resilienza – Sistemi di gestione per la continuità operativa - Requisiti
[12]	ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
[13]	UNI ISO 45001:2018 – Sistema di gestione della salute e della sicurezza sul lavoro
[14]	Campo di Applicazione SGI
[15]	UNI PdR 125:2022 Linee guida sul sistema di gestione per la parità di genere che prevede l'adozione di specifici KPI (Key Performances Indicator - Indicatori chiave di prestazione) inerenti alle Politiche di parità di genere nelle organizzazioni

RIF.	*Nome*
[16]	L. nr. 162/2021 Modifiche al codice di cui al D. Lgs. 11 aprile 2006, n. 198, e altre disposizioni in materia di pari opportunità tra uomo e donna in ambito lavorativo
[17]	Ruoli e Responsabilità per il SGIG
[18]	Parità di Genere - Piano Strategico del Gruppo Infordata
[19]	SGIG_PO.GS-SA8000&PG_Procedura Gestione delle Segnalazioni - SA8000 & Parità di Genere

Termini e definizioni

Termine	Definizione
SGIG	Sistema di Gestione Integrato di Gruppo
SGI	Sistema di Gestione Integrato
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SGQ	Sistema di Gestione della Qualità
SGS	Sistema di Gestione dei Servizi
SGA	Sistema di Gestione Ambientale
SGRS	Sistema di Gestione della Responsabilità Sociale
BCMS	Sistema di Gestione per la Business Continuity
SGSSL	Sistema di Gestione per la Salute e la Sicurezza sul Lavoro
Gruppo Infordata	Qui inteso costituito dalle seguenti aziende: Infordata S.p.A, Eurolink S.r.l., Technis Blu S.r.l.
Whistleblowing	Fondamentale strumento di compliance aziendale, tramite il quale i dipendenti oppure terze parti (per esempio un fornitore o un cliente) di un'azienda possono segnalare, in modo riservato e protetto, eventuali illeciti riscontrati durante la propria attività
IPCP	Infordata Private Cloud Platform

Sommario

1 Scopo

Il Gruppo Infordata è convinto che il processo di miglioramento continuo costituisca l'elemento fondamentale per raggiungere l'eccellenza nel coniugare la crescita aziendale, con elevati standard di qualità ed efficienza dei servizi erogati, il rispetto dell'ambiente, la tutela della salute e sicurezza dei lavoratori. I modelli adottati dal Gruppo Infordata assegnano al Cliente un ruolo primario: la piena comprensione delle esigenze e la progettazione di soluzioni personalizzate garantiscono il raggiungimento di obiettivi di eccellenza.

Il Gruppo Infordata ha pertanto adottato la scelta strategica di porre la massima attenzione alle esigenze dei propri clienti, migliorando la comprensione dei loro bisogni e monitorando costantemente il servizio ed i processi interni affinché vengano mantenute le prestazioni monitorate attraverso indicatori chiave di performance (KPI), in linea con gli obiettivi aziendali.

L'impegno del Gruppo Infordata si è concretizzato nell'istituzione di un Sistema di Gestione Integrato di Gruppo (SGIG) per: la Gestione della Qualità (SGQ), dell'Ambiente (SGA), della Sicurezza delle Informazioni (SGSI), della gestione dei Servizi (SGS), della Responsabilità Sociale (SGRS) e della Salute e Sicurezza sul Lavoro (SGSSL).

L'impegno della Infordata Education S.r.l. (non più parte del Gruppo Infordata, ma società a cui continua ad applicarsi tutta la documentazione del SGIG), invece, si è concretizzato nell'istituzione del solo Sistema di Gestione per la Qualità (SGQ).

Il Gruppo Infordata in relazione alla decisione di istituire il suo SGIG definisce la presente informazione documentata "**Politiche per il SGIG"**, che:

- ✓ stabilisce, implementa, attua, controlla, riesamina, mantiene e migliora in modo continuo il proprio SGIG e i correlati SGI aziendali;
- ✓ si è dotata di un sistema di valutazione e trattamento dei rischi e delle opportunità (Rif. [3]) adatto alle proprie necessità e agli schemi di certificazione in suo possesso;
- ✓ dimostra la sua capacità di fornire costantemente prodotti e servizi che soddisfino i requisiti legali e normativi applicabili nonché quelli forniti dal Cliente;
- ✓ destina adeguate risorse per il raggiungimento degli obiettivi pianificati;
- ✓ persegue la soddisfazione del Cliente attraverso l'effettiva applicazione del SGIG.

Tali Politiche vengono approvate, riviste e aggiornate periodicamente in maniera congiunta da tutti e quattro le Direzioni di Eurolink S.r.l., Infordata S.p.A., Technis Blu S.r.l. e Infordata Education S.r.l.. Inoltre le politiche riferite ai diversi Sistemi di Gestione sono da intendersi applicabili a seconda delle certificazioni ottenute dalle singole aziende rispetto ciascun Sistema di Gestione.

I contenuti di tali Politiche devono essere diffusi a tutte le parti interessate esterne ed interne.

2 Principi

I principi del SGIG sono i seguenti.

1. Orientamento al Cliente: il Gruppo dipende dai propri Clienti e pertanto cerca di soddisfare le loro esigenze presenti e future, e soddisfare, oltre quelli legali e normativi, i loro requisiti nonché mirare a superare le loro stesse aspettative.
2. Coinvolgimento del personale: il Gruppo è consapevole che le persone, a tutti i livelli, costituiscono l'essenza dell'organizzazione ed il loro pieno coinvolgimento – senza alcuna discriminazione e con la massima libertà di espressione – permette di porre le loro capacità al servizio dell'organizzazione.
3. Chiara definizione dei ruoli e responsabilità: il Gruppo definisce in modo chiaro le responsabilità del personale e degli utenti in relazione ai requisiti del SGIG e dei SGI aziendali.
4. Trasparenza: il Gruppo definisce e rende pubblici i propri principi etici e di comportamento mediante la pubblicazione del "Codice Etico" di Gruppo ed i singoli codici etici aziendali.
5. Approccio per processi: il Gruppo favorisce un approccio per processi al fine di perseguire i risultati desiderati con maggior efficienza.
6. Miglioramento continuo: il miglioramento continuo delle prestazioni complessive è un obiettivo permanente del Gruppo.
7. Decisioni basate su dati di fatto: il Gruppo basa le proprie decisioni sull'analisi di dati e di informazioni e sulle risultanze dei processi di analisi del rischio.
8. Rapporti di reciproco beneficio con i fornitori: il Gruppo ed i suoi fornitori sono interdipendenti ed un rapporto di reciproco beneficio migliora, per entrambi, la capacità di creare valore.

3 Obiettivi - Impegno delle Direzioni

Le Direzioni del Gruppo hanno deciso di garantire e sostenere il SGIG strutturato secondo quanto indicato in Rif. [1] ed in conformità delle norme e dei regolamenti in Rif. [2], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13]. A tale scopo definiscono i seguenti obiettivi per le seguenti politiche.

4 Politica Integrata di Gruppo

Le Direzioni del Gruppo per raggiungere il livello di qualità desiderato e definito tramite obiettivi e traguardi stabiliti annualmente nel Riesame della Direzione, perseguono la soddisfazione e la fidelizzazione dei propri clienti e dei propri stakeholders ponendo attenzione a:

- ✓ garantire che la politica sia appropriata alle finalità dell'organizzazione;
- ✓ assicurare le autorità e responsabilità per i propri sistemi di gestione;
- ✓ assicurare il rispetto di tutte le normative internazionali cogenti e legali applicabili;
- ✓ aumentare costantemente la soddisfazione dei Clienti ponendo l'attenzione sia ai requisiti espliciti, ovvero quelli espressamente riportati nei contratti di fornitura, che inespressi;

- ✓ mantenere le certificazioni migliorando il SGIG e aggiornandolo a seguito dei cambiamenti normativi periodici, anche con l'attuazione di progetti interni volti all'ottimizzazione dei processi in essere;
- ✓ ottenere nuove certificazioni tenendo in considerazione le strategie del business di Gruppo;
- ✓ aumentare un'attività diffusa di aggiornamento dei processi e dei servizi del sistema organizzativo, al fine di consolidare e rafforzare la qualità delle operazioni e dei controlli;
- ✓ incrementare il fatturato annuale puntando sull'aumento del numero di commesse/attività;
- ✓ promuovere uno sforzo costante teso al coinvolgimento di tutto il personale nelle attività e nelle attenzioni necessarie a realizzare un continuo incremento dell'efficienza e dell'eccellenze aziendali;
- ✓ stabilire un rapporto di collaborazione e fiducia con i fornitori atto a raggiungere l'obiettivo comune di erogare servizi e prodotti che soddisfino le esigenze del Cliente;
- ✓ adottare una attenta valutazione nelle diverse Aziende del gruppo definendo congrui obiettivi con cui confrontarsi criticamente e attraverso i quali ragionare in maniera più compiuta sui miglioramenti da adottare;
- ✓ rispettare i requisiti cogenti e normativi applicabili ai propri prodotti e servizi prestando in tutte le Aziende del gruppo la massima attenzione alla protezione dei dati personali in proprio possesso trattandoli secondo i principi di liceità, correttezza, trasparenza, raccogliendoli in modo pertinente e non eccedenti rispetto agli scopi e conservandoli adeguatamente, proteggendoli attraverso le idonee misure tecniche ed organizzative determinate sulla base del rischio del trattamento a cui i dati sono sottoposti, come previsto dal vigente GDPR;
- ✓ seguire il perseguimento del miglioramento continuo dei processi e delle prestazioni, coinvolgendo le parti interessate, valutando il contesto nel quale opera l'organizzazione al fine di identificarne i rischi e le opportunità;
- ✓ adottare misure tecniche e organizzative volte ad assicurare la salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite promovendo un processo di miglioramento continuo al fine di elevare il livello di sicurezza complessivo di tutte le Aziende del gruppo;
- ✓ proteggere le risorse informatiche aziendali attraverso la selezione e l'applicazione di appropriate misure precauzionali che favoriscano il raggiungimento degli obiettivi aziendali;
- ✓ diffondere la cultura del risk management per migliorare costantemente le conoscenze e la gestione dei rischi in quanto componente strategica per il successo e causa di potenziali impatti che potrebbero minare la stabilità e la continuità del business;
- ✓ fornire un ambiente di lavoro sano, sicuro, non discriminatorio e stimolante basato sul rispetto e la fiducia nei lavoratori allo scopo di facilitare il raggiungimento degli obiettivi di lungo periodo del Gruppo Infordata.

4.1 Politica per la Qualità – SGQ

Le Direzioni del Gruppo stabiliscono i seguenti obiettivi validi per i propri SGQ:

- ✓ garantire attenzione focalizzata sul Cliente e sulle parti interessate finalizzata a comprendere le necessità dei Clienti e pianificare le proprie attività per soddisfarle appieno;

- ✓ promuovere un approccio per processi indentificando le diverse attività della propria organizzazione come processi da pianificare, controllare e migliorare costantemente e attiva al meglio le risorse per la loro realizzazione;
- ✓ aumentare il livello di coinvolgimento del personale e degli stakeholder;
- ✓ migliorare l'efficienza interna;
- ✓ attuare un approccio risk-based thinking (RBT) al fine di valutare e minimizzare i rischi di insuccessi tecnici e commerciali;
- ✓ promuove lo sviluppo delle professionalità interne e l'attenta selezione delle collaborazioni esterne al fine di dotarsi di risorse umane competenti e motivate.

4.2 Politica per la sicurezza delle informazioni

Le Direzioni del Gruppo stabiliscono i seguenti obiettivi validi per i propri SGSI:

- ✓ Supportare il management e tutto il personale a raggiungere un livello di conoscenza, di consapevolezza e abilità per consentire di ridurre al minimo i rischi per possibili danni scaturiti da eventi avversi alla sicurezza delle informazioni;
- ✓ Garantire e proteggere le informazioni relative al business del Gruppo comprese tutte le informazioni dei clienti e personale interno salvaguardando la riservatezza, integrità e disponibilità;
- ✓ Stabilire ed attuare le misure di sicurezza per la protezione delle informazioni relative al campo di applicazione del Gruppo da abusi, frodi, uso indebito e furto;
- ✓ Integrare all'interno dei propri processi di sviluppo delle applicazioni i principi di ingegnerizzazione sicura dei sistemi nel rispetto delle specificità delle Aziende;
- ✓ Attuare il mascheramento dei dati (c.d. Data Masking) laddove necessario sulla base della legislazione applicabile nonché dei requisiti aziendali e/o del Cliente;
- ✓ miglioramento continuo del SGSI.

4.2.1 Politica per i servizi Cloud – (Infordata S.p.A. ed Eurolink S.r.l.)

In estensione agli obiettivi descritti nel precedente par. 4.2 "Politica per la sicurezza delle informazioni", conformemente alla ISO/IEC 27017 (Rif. [9]) per i Servizi Cloud ed alla ISO/IEC 27018 (Rif. [8]) per la Protezione delle Informazioni Personali Identificabili (PII) nel Cloud Pubblico, Infordata S.r.l. ed Eurolink S.r.l. stabiliscono i seguenti obiettivi:

- ✓ che le informazioni siano protette da accessi non autorizzati, anche ricorrendo alla crittografia di dati e comunicazioni, nel rispetto della riservatezza e siano disponibili agli utenti autorizzati quando ne hanno bisogno;
- ✓ che il Personale riceva addestramento e aggiornamento sulla sicurezza delle informazioni con particolare riferimento agli ambienti Cloud;
- ✓ che nell'ambito dei servizi Cloud erogati, gli asset dei Clienti dei servizi verranno censiti e gestiti;
- ✓ che le informazioni non vengano rivelate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;

- ✓ che vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- ✓ che tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano comunicati ed esaminati da tutte le parti interessate, interne ed esterne;
- ✓ che vengano garantiti le opportune segregazioni degli ambienti e delle informazioni relative ai singoli Clienti dei servizi Cloud;
- ✓ che le reti virtuali vengano configurate in modo tale da assicurare la Riservatezza delle informazioni così come previsto per le reti fisiche;
- ✓ che il raggiungimento della conformità alle leggi relative alla protezione dei dati personali con particolare riguardo ai dati forniti dai Clienti nell'ambito dei servizi Cloud;
- ✓ garantire la connettività ai servizi offerti in cloud per i Clienti;
- ✓ scelta di fornitori qualificati nell'ottica della qualità dei servizi Cloud offerti.

4.2.2 Politica per la sicurezza delle informazioni nelle relazioni con i fornitori

L'Organizzazione adotta e mantiene aggiornato un sistema di Gestione al fine di garantire gli aspetti di sicurezza inerenti gli accessi ai beni da parte dei fornitori esterni.

a. Politica per la sicurezza delle informazioni nei rapporti con i fornitori

Al fine di identificare e mitigare i rischi potenziali derivanti dall'accesso dei fornitori agli asset aziendali, il Gruppo Infordata ha stabilito e applica opportune politiche e procedure che prevedono:

- ✓ l'identificazione e la documentazione di tutti i fornitori (ad es. fornitori di servizi, produttori di componenti, ecc.) che possono aver accesso alle informazioni;
- ✓ la condivisione con i fornitori dei principi della sicurezza delle informazioni;
- ✓ l'identificazione delle informazioni e delle modalità di accesso dei fornitori, nonché le modalità di monitoraggio e controlli di tali accessi;
- ✓ opportuni controlli per monitorare il rispetto da parte dei fornitori dei requisiti di sicurezza concordati (ad es. attraverso riesami di terze parti o validazioni dei prodotti);
- ✓ le modalità di gestione degli incidenti, sia reali che presunti, incluse le specifiche responsabilità di entrambe le parti, legati all'accesso dei fornitori alle informazioni dell'organizzazione;
- ✓ le modalità di gestione delle informazioni e dei servizi forniti dalle terze parti al fine di garantire la loro disponibilità (ad es. in termini di backup, continuità operative, etc...);
- ✓ un'adeguata formazione al personale interno coinvolto nella gestione delle relazioni con i fornitori e nelle attività di acquisizione/fornitura di informazioni e servizi da/a terze parti;
- ✓ la gestione delle informazioni, dei servizi e dei dispositivi che contengono informazioni che vengono movimentati al fine di garantire gli aspetti di sicurezza durante la fase di transito.

b. Indirizzare la sicurezza all'interno degli accordi con i fornitori

Al fine di indirizzare gli aspetti di sicurezza ed evitare eventuali incidenti ed incomprensioni nella salvaguardia di disponibilità, integrità e disponibilità delle informazioni e dei servizi trattati anche da fornitori esterni, il Gruppo Infordata ha stabilito che tra l'organizzazione e le terze parti devono essere stipulati e documentati appositi contratti che prevedono opportune clausole di sicurezza.

Tali accordi (vedi "Non Disclosure Agreement/Obbligo di Riservatezza e Confidenzialità") contengono le responsabilità sia dell'organizzazione che del fornitore nel raggiungere e soddisfare i requisiti della sicurezza delle informazioni e tengono in considerazione:

- ✓ descrizione delle informazioni e relative modalità di accesso o fornitura delle stesse;
- ✓ classificazione delle informazioni, eventualmente creando una mappatura tra i livelli di classificazione dell'organizzazione e quelli del fornitore;
- ✓ eventuali requisiti legali e normative (ad es. sulla protezione delle informazioni, su marchi, copyright o qualunque altro diritto di proprietà intellettuale ed industriale, ecc.);
- ✓ gli obblighi di ciascuna parte per l'implementazione dei controlli di sicurezza definiti nell'accordo contrattuale o di fornitura (ad es. sul controllo degli accessi, sulle modalità di monitoraggio e auditing, ecc.);
- ✓ le regole stabilite per l'utilizzo delle informazioni a cui si ha accesso;
- ✓ eventuali liste di distribuzione di persone/collaboratori autorizzati ad accedere o ricevere le informazioni oggetto dell'accordo, o specifiche procedure per gestire l'aggiunta o la rimozione di persone/collaboratori a tali liste di distribuzione;
- ✓ ulteriori politiche di sicurezza delle informazioni definite nel contratto di fornitura;
- ✓ requisiti e procedure per la gestione degli incidenti di sicurezza delle informazioni;
- ✓ eventuali esigenze formative per il personale che accede alle informazioni e ai servizi oggetto di fornitura;
- ✓ le responsabilità di eventuali sub fornitori, inclusi i controlli necessari che devono essere implementati;
- ✓ la possibilità per l'organizzazione di effettuare audit sui fornitori;
- ✓ i requisiti e le modalità di rescissione delle parti coinvolte;
- ✓ l'obbligo per le terze parti di fornire report periodici sull'efficacia dei controlli;
- ✓ l'obbligo per i fornitori di essere conformi ai requisiti di sicurezza dell'organizzazione.

c. Filiera di fornitura per l'ICT

Gli accordi con i fornitori (vedi "Non Disclosure Agreement/Obbligo di Riservatezza e Confidenzialità") prevedono inoltre i requisiti per indirizzare i possibili rischi alla sicurezza delle informazioni derivanti dall'accesso e dalla comunicazione delle informazioni del Gruppo Infordata durante la filiera di fornitura.

4.3 Politica per la gestione del servizio - SGS

Le Direzioni del Gruppo stabiliscono i seguenti obiettivi validi per i propri SGS:

- ✓ fornire ai propri Clienti servizi che costituiscano un forte valore facilitando i risultati che i Clienti desiderano raggiungere senza sostenere gli specifici rischi e costi;
- ✓ definire, mantenere e migliorare il catalogo dei servizi in aderenza alle esigenze dei propri clienti, progettando e fornendo servizi anche innovativi e che creino per loro sempre maggior valore;
- ✓ garantire ai propri clienti la costante disponibilità di persone, processi e tecnologie a supporto dei servizi erogati e nel rispetto dei Livelli di Servizio definiti (SLA);

- ✓ assicurare che il Gruppo Infordata possa continuare le attività di business anche in caso di avverse situazioni;
- ✓ definire, attuare e monitorare gli obiettivi per quanto riguarda i piani di: gestione del servizio, di continuità, di disponibilità, di capacità e di rilascio/messa in funzione, così come previsto dalla norma in riferimento;
- ✓ assicurare il miglioramento continuo dei servizi, processi, risorse, capability per garantire l'efficacia e l'efficienza quale Service Provider presente in un mercato competitivo;
- ✓ sviluppare accordi, partnership con Fornitori, terze parti allo scopo di garantire un catalogo servizi più ampio e una maggiore competitività finalizzata alla soddisfazione del cliente e delle parti interessate.

4.4 Politica Ambientale - SGA

Le Direzioni del Gruppo stabiliscono i seguenti obiettivi validi per i propri SGA:

- ✓ migliorare l'impatto ambientale sulla comunità (acqua, aria, suolo e sottosuolo), correlati al suo contesto operativo e al territorio in cui opera;
- ✓ definire e valutare, mediante il processo di miglioramento continuo, obiettivi ambientali tesi alla protezione dell'ambiente ed alla prevenzione dell'inquinamento pertinenti al contesto aziendale;
- ✓ tenere sotto controllo la gestione dei rifiuti e lo smaltimento dei prodotti al termine del loro ciclo di vita, nonché del consumo di risorse energetiche e naturali al fine di ridurne gli sprechi.

4.5 Politica per la Responsabilità Sociale - SGRS

Infordata S.p.A. stabilisce i seguenti principi validi per il proprio SGRS:

- ✓ rispettare i principi di responsabilità sociale espressi dalle Convenzioni e Raccomandazioni ILO, dalle dichiarazioni internazionali delle Nazioni Unite, dalle Direttive e dai Regolamenti Europei e dalle Leggi nazionali;
- ✓ non utilizzare né dare sostegno in nessun caso al lavoro infantile, promuovendo piuttosto l'alternanza "scuola-lavoro" ed accogliendo i ragazzi durante il loro periodo di studi, in modo da consentire un approccio corretto con il mondo del lavoro;
- ✓ non utilizzare né dare sostegno al lavoro forzato o obbligato, piuttosto interessarsi dei propri lavoratori perché non si creino situazioni di dipendenza tali da costringere il lavoratore a permanere contro la sua volontà all'interno dell'azienda;
- ✓ garantire che le attività lavorative si svolgano in ambienti di lavoro salubri ed in condizioni di sicurezza, riducendo al minimo i rischi associati alla salute e alla sicurezza nei luoghi di lavoro, garantendo procedure e misure di protezione idonee ed efficaci, anche attraverso la consultazione e la partecipazione dei lavoratori stessi;
- ✓ garantire il diritto alla contrattazione collettiva senza alcuna ripercussione sul personale, promuovendo la conoscenza del Contratto Collettivo Nazionale del Lavoro e dei diritti dei lavoratori e consentendo loro di partecipare e organizzare sindacati senza alcuna forma di ritorsione o discriminazione nei confronti dei rappresentanti sindacali;

- ✓ respingere ogni forma di discriminazione e promuovere le pari opportunità, migliorando l'inclusione di tutto il personale per tutto il percorso lavorativo dalla selezione del personale, all'assunzione, all'accesso alla formazione, alle promozioni, al licenziamento e al pensionamento;
- ✓ trattare chiunque, in particolare il proprio personale, con dignità e rispetto, senza fare ricorso ad alcuna forma di coercizione fisica o mentale, ricorrendo a provvedimenti disciplinari nel pieno rispetto del contratto di lavoro e del codice etico applicati;
- ✓ applicare con attenzione i contratti collettivi nazionali di lavoro, con particolare riferimento all'orario di lavoro, ai livelli retributivi, alla regolamentazione di ferie e pause di riposo, nonché agli straordinari.

4.6 Politica per la Protezione dei Dati Personali

Con la politica per la protezione dei data personali le Direzioni del "Gruppo Infordata " intendono proteggere le informazioni e i dati personali gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste (Rif. [7]) dal Regolamento (UE) 27/04/2016, n. 679 e dal Decreto Legislativo n. 196 del 30/06/2003, così come novellato dal Dlgs. 101 del 10 agosto 2018 (nel seguito complessivamente "Regolamento").

Le Direzioni riconoscono la propria responsabilità e si impegnano a proteggere i dati personali che gli utenti affidano all'azienda da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, il gruppo si avvale del proprio "SGSI", di una serie di tecnologie e procedure aziendali di protezione. La protezione dei dati personali, come prevista dal Regolamento, sarà attuata secondo le regole Privacy by design e Privacy by default.

La Infordata Education riconosce la propria responsabilità e si impegna a proteggere i dati personali che gli utenti affidano all'azienda da perdita, uso improprio o accesso non autorizzato. Infordata Education si avvale di una serie di tecnologie e procedure aziendali di protezione. La protezione dei dati personali, come prevista dal Regolamento, sarà attuata secondo le regole Privacy by design e Privacy by default.

La presente politica si applica a tutti gli organi e i livelli del "Gruppo Infordata". La sua attuazione è obbligatoria per tutto il personale ed è inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno coinvolto con il trattamento di dati personali. Il "Gruppo Infordata" consente la comunicazione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività e per il rispetto delle regole e delle norme vigenti.

Le Aziende del "Gruppo Infordata" hanno istituito e mantengono aggiornato: un registro delle attività di trattamento, una valutazione di impatto sulla protezione dei dati che consente di acquisire consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati mediante la quale si determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

I principi generali della gestione della sicurezza delle informazioni si basano su alcuni punti fondamentali così come previsto anche dai "SGSI" delle singole aziende, in particolare:

- ✓ Esiste un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno è individuato un responsabile;

- ✓ Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza e integrità coerenti e appropriati;
- ✓ Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi è sottoposto a una procedura d'identificazione e autenticazione;
- ✓ Sono definite delle procedure per l'utilizzo sicuro dei beni e delle informazioni aziendali;
- ✓ È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
- ✓ Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza;
- ✓ È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
- ✓ È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- ✓ È predisposto un piano di continuità che permette 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;
- ✓ Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

4.7 Politica per la Salute e Sicurezza sul Lavoro - SGSSL

Infordata S.p.A. e Eurolink S.r.l. stabiliscono i seguenti principi validi per i propri SGSSL:

- ✓ fornire condizioni di lavoro sicure e salubri per la prevenzione di lesioni e malattie correlate al lavoro congrue alle dimensioni, al contesto delle Organizzazioni coinvolte e alla natura specifica di possibili rischi e opportunità;
- ✓ fissare gli obiettivi correlati;
- ✓ impegnarsi ad eliminare i pericoli e a ridurre i rischi per la salute e la sicurezza;
- ✓ migliorare in modo continuo il relativo sistema di gestione
- ✓ impegnarsi a garantire la consultazione e partecipazione dei lavoratori e, ove istituiti, dei rappresentanti dei lavoratori.

4.8 Politica per la Parità di Genere

Il Gruppo Infordata ha nominato un Organo per la Parità di Genere (i cui componenti sono pubblicizzati per mezzo di comunicazione degli Organigrammi aziendali) al fine della corretta attuazione della relativa politica, allineata alla Legge n 162 del 5 novembre 2021 (Rif. [16]) ed alla Prassi di riferimento UNI PdR 125:2022 (Rif. [15]).

La Infordata S.p.A. (Capogruppo), così come Technis Blu S.r.l. ed Eurolink S.r.l., operano cercando di offrire pari opportunità a tutti i dipendenti, senza discriminazioni in alcun aspetto del rapporto di lavoro basate su:

- razza;
- religione;
- colore;
- etnia;
- nazione di origine;
- età;
- invalidità;
- tendenze sessuali;
- opinioni politiche;
- sesso;
- stato civile.

Per tutto ciò che riguarda l'impiego, l'assunzione, la retribuzione e i benefit, le promozioni, i trasferimenti e la risoluzione del rapporto di lavoro, le persone sono trattate in modo equo, in funzione della loro capacità di soddisfare i requisiti e gli standard previsti nei vari ruoli in cui sono coinvolte.

Nessun dipendente è sottoposto a violenza o molestia fisica, sessuale, razziale, psicologica, verbale o di altro genere. L'azienda assicura che sono attuate procedure atte a rilevare i casi di infrazione, per essere all'altezza di questo standard e intervenire in modo rapido ed efficace.

Di seguito i comportamenti proibiti da questa politica.

1. **Discriminazione.** Costituiscono una violazione di questa politica:
   - la discriminazione nell'offerta di opportunità di impiego, benefit o privilegi;
   - la creazione di condizioni di lavoro discriminatorie
   - l'uso di standard di valutazione discriminatori nell'ambito del rapporto di lavoro se la discriminazione è basata, del tutto o in parte, sui dati particolare che rivelano gli aspetti elencati al par. di cui sopra;

   È mandatorio per le società del Gruppo Infordata il rispetto integrale della legislazione in materia, comprese le leggi sulla discriminazione;

   La discriminazione messa in atto in violazione di questa politica di pari opportunità viene punita con severe sanzioni, che possono arrivare fino alla risoluzione del rapporto di lavoro.

2. **Molestie.** Questa politica proibisce le molestie di ogni genere, e le eventuali violazioni sono adeguatamente perseguite dall'azienda. Viene definita molestia una condotta, verbale o fisica, il cui intento è la minaccia, l'intimidazione o la coercizione. Si considerano molestia, inoltre, le espressioni verbali di scherno (comprese le ingiurie riferite a razza ed etnia) che, secondo la persona che le subisce, si ripercuotono sulla sua capacità di svolgere il suo lavoro.
   Nelle molestie, rientrano quelle di tipo:
   - sessuale, in qualsiasi forma. Vengono definite molestie sessuali le avances non gradite, la richiesta di favori sessuali ed altri comportamenti verbali o fisici di natura sessuale, se la sottomissione o il rifiuto vengono usati per influenzare decisioni nell'ambito del lavoro, o se tali comportamenti hanno lo scopo o l'effetto di creare un ambiente di lavoro intimidatorio, ostile od offensivo.

4.8.1 Monitoraggio e Reporting

È compito del Gruppo Infordata assicurare l'osservanza di tutte le leggi sulla parità applicabili e di far sì che i dipendenti abbiano accesso a procedure sulla discriminazione formali e non esposte a ritorsione per riferire le infrazioni.

In fase di implementazione il sistema di Whistleblowing, il quale permette segnalazioni di qualsiasi genere, anche in forma anonima.
Al momento, il Gruppo Infordata, all'indicatore nr. 2 dell'Area "Cultura & Strategia" della UNI PdR 125:2022 (Rif. [15]), risponde con l'estensione alla Parità di Genere della procedura SGIG_PO.GSS-SA8000&PO_Procedura Gestione delle Segnalazioni - SA8000 & Parità di Genere (Rif. [19]).

Nell'ambito del nostro impegno per la promozione della parità di genere, terremo monitorati i risultati ottenuti che saranno mantenuti dall'ufficio HR del Gruppo per eventuali consultazioni.

L'attenzione ai temi relativi alla parità di genere da parte del Gruppo Infordata è radicata, da parte della Direzione, su tutti i manager: da sempre non sono mai state necessarie indicazioni su comportamenti da tenere nelle varie fasi aziendali (dall'assunzione ai riconoscimenti/premi) e per la gestione delle risorse in generale.

Tutta la linea manageriale è perfettamente preparata alla sana gestione dei vari aspetti legati ai vari pregiudizi e stereotipi legati al genere. Tutti conoscono il nostro Codice Etico di Gruppo, correttamente applicato, soprattutto sui temi e sulle modalità operative adottati dall'organizzazione, per garantire l'efficacia della politica per la parità di genere.

4.8.2 Il Piano Strategico

Infordata S.p.A., Eurolink S.r.l. e Technis Blu S.r.l., data l'avvenuta uniformazione dell'Ufficio del Personale, adottano lo stesso Piano Strategico in termini di Parità di Genere (Rif. [18]): quest'ultimo è elaborato secondo il requisito 6.3 della UNI PdR 125:2022 (Rif. [15]) e di seguito descritto per macro-temi.

1. **Selezione ed assunzione**. Tutte le nostre procedure di selezione ed assunzione non prevedono alcuna regola che indichi delle direttive sulla disparità di genere e tutte le nostre ricerche di mercato sono indirizzate in modo equo a candidati di entrambi i sessi e genere a partire dalle richieste di assunzione che sono neutre rispetto al genere. Tutte le persone addette ai colloqui sono allineate sul fatto del non menzionare mail temi come matrimonio, gravidanza e temi di salute specifici. Garantita da parte dell'Ufficio del Personale del Gruppo Infordata anche un'analisi del Turnover.
2. **Gestione della carriera**. La politica aziendale, normata anche da procedure specifiche, definisce l'assoluta mancanza di discriminazione e le pari opportunità nello sviluppo professionale e nelle promozioni, che si basano solo su aspetti meritocratici sulla base dei vari livelli professionali; c'è una continua attenzione nel cercare di bilanciare, nelle posizioni di leadership aziendale, le specificità di genere.

Tutte le persone sono coinvolte nelle opportunità di carriera e nello sviluppo professionale in tutta l'organizzazione e sempre basandosi sugli aspetti meritocratici.

3. **Equità salariale**. Il Bilancio di Sostenibilità (redatto al momento per Infordata S.p.A. e Technis Blu S.r.l.), nel quale i nostri dipendenti sono identificati come Stakeholders, mostra in modo trasparente la situazione salariale, per livello e per tutti gli elementi del personale necessari al confronto tra i diversi generi. Questi dati sono disponibili anche a tutto il personale così come le informazioni relative alla situazione organizzativa diffusa periodicamente a tutti i dipendenti.
   Tutte le politiche salariali sono estremamente trasparenti nella loro applicazione concreta attraverso l'attribuzione di benefit, bonus e in generale nella predisposizione e attuazione di programmi di welfare aziendale.
   Dai contenuti del documento Ruoli e Responsabilità per il SGI (Rif. [17]), inoltre, si può evincere l'assenza di discriminazioni di genere circa l'attribuzione dei ruoli e delle responsabilità aziendali.

   - **Nota**: rileva in tal contesto la Dichiarazione obbligatoria che viene trasmessa ogni anno (per aziende costituite da più di 50 dipendenti) dalle Società del Gruppo Infordata al Ministero del Lavoro e delle Politiche Sociali attraverso il relativo sito istituzionale.

3. **Genitorialità e cura**. Il Gruppo Infordata applica correttamente quanto previsto dalla legge ed i re-inserimenti delle persone in maternità o paternità sono sempre condivise con il personale ed opportunamente supportati da corsi di formazione integrativi nel caso se ne evidenzi il bisogno.

   Rispetto a necessità legate alla maternità/paternità, possono essere rivisti o stipulati gli accordi individuali di smart-working nonché fare richiesta di un part-time reversibile.

   In occasione dei rientri dalla maternità/paternità, è possibile prendere parte anche a corsi di formazione specifica di tipo integrativo: il dipendente comunicherà al proprio Responsabile la necessità di essere supportato in tal senso (Rif.

4. **Conciliazione dei tempi vita-lavoro**. Spinto da esigenze correlate alla pandemia da Covid-19, il Gruppo Infordata ha rafforzato l'utilizzo dello Smart Working nei termini di legge previsti e secondo quanto concordato coi dipendenti. Restano ferme le eccezioni legate a richieste del Cliente che prevedano svolgimento di attività necessariamente on-site.

   Tutte le richieste di lavoro part-time, inoltre, vengono prese in considerazione e valutate in relazione alle necessità di mercato favorendo sempre il dipendente, di qualsiasi genere.

   Ad ogni modo, l'orario di ufficio è flessibile e la gestione è improntata nella massima fiducia posta nei confronti dei dipendenti non avendo mai istituito il cartellino orario.

   Un esempio di flessibilità può essere rappresentato dalla pianificazione delle riunioni di lavoro, nel qual caso, la scelta della data, della fascia oraria e della modalità di esecuzione (remoto/on-site) avvengono favorendo il personale partecipante, laddove possibile.

5. **Prevenzione su ogni forma di abuso fisico, verbale, sul luogo di lavoro.** Sul tema in oggetto, la politica aziendale è estremamente severa e l'applicazione del nostro Codice Etico di Gruppo, nonché l'adozione del Modello Organizzativo 231, garantiscono, per tutti i lavoratori, la corretta attuazione dei sani principi rispetto al proprio luogo di lavoro. Non si prevedono piani speciali perché non sono accettate deroghe: vige, quindi, il divieto assoluto di qualsiasi forma di abuso fisico, verbale, digitale.

Infordata S.p.A. accresce la protezione dei lavoratori in tal contesto, rispettando i requisiti della certificazione SA8000:2014 posseduta.
Inoltre, è in fase di implementazione il sistema di Whistleblowing, il quale permette segnalazioni di qualsiasi genere, anche in forma anonima.
Al momento, pertanto, il Gruppo Infordata, all'indicatore nr. 2 dell'Area "Cultura & Strategia" della UNI PdR 125:2022 (Rif. [15]), risponde con l'estensione alla Parità di Genere della procedura SGI_PO.GSSA800_Gestione Segnalazioni SA8000 (Rif. [19]).
Sempre in forma anonima, è prevista una survey motivazionale e sui comportamenti della linea manageriale attraverso la quale è possibile di individuare eventuali situazioni esistenti potenzialmente compromettenti il clima aziendale.

4.9 Politica per la Continuità Operativa – BCMS

La Direzione della Società del Gruppo Infordata Eurolink S.r.l. stabilisce la propria Politica di continuità aziendale allineata al suo Core Business coi correlati e seguenti obiettivi da perseguire:

- ✓ rispettare tutti i requisiti applicabili, cogenti e derivanti dallo schema ISO di riferimento;
- ✓ garantire una comunicazione trasparente interna ed esterna, al fine di non bloccare i processi aziendali tutti e non solo quelli produttivi;
- ✓ formare e sensibilizzare il proprio capitale umano rendendolo edotto rispetto quanto i comportamenti del singolo siano importanti nel rispetto dei requisiti di cui sopra, della garanzia della continuità e del miglioramento continuo di quest'ultima;
- ✓ garantire ai propri Clienti la continua disponibilità di persone, processi e tecnologie a supporto dei servizi erogati;
- ✓ garantire, laddove possibile, sempre lo Smart Working quale modalità di esecuzione dell'attività lavorativa;
- ✓ effettuare una valutazione dei rischi in modalità preventiva al fine di poter individuare misure da adottare in caso di eventi dannosi aventi ad oggetto i principali servizi definiti critici;
- ✓ assicurare che l'Azienda non arresti il proprio Core Business in caso di situazioni avverse;
- ✓ definire, attuare, monitorare ed eventualmente aggiornare il proprio piano di continuità seguendo l'evoluzione aziendale ed, in particolare, il Core Business;
- ✓ garantire la sostituibilità delle figure apicali attraverso una matrice definita;
- ✓ assicurare il miglioramento continuo dei servizi, processi, risorse, capability per garantire l'efficacia e l'efficienza dei servizi erogati.

5 Attuazione del SGIG

Il SGIG è inteso come l'insieme di vari elementi: politiche, obiettivi, piani e processi; esso viene costituito e realizzato per raggiungere gli obiettivi relativi ai sistemi di gestione per cui le singole aziende sono certificate.

All'interno del Gruppo ogni azienda, mediante la propria informazione documentata **Campo di Applicazione SGI** (Rif. [14]), definisce l'ambito all'interno del quale vengono posti in essere processi e attività.

Tutto il personale del Gruppo, i fornitori o terze parti sotto contratto, che rientrano nei campi di applicazione aziendali, sono responsabili dell'attuazione della presente politica con il supporto delle Direzioni che l'hanno approvata.

Le Direzioni del Gruppo sostengono i principi ed obiettivi per il SGIG e supportano in modo pieno e completo il programma per la sua attuazione, mantenimento e miglioramento fornendo le risorse necessarie al raggiungimento di tali scopi. Le Direzioni approvano ed emettono il presente documento di **Politiche per il SGIG**, che costituisce il documento programmatico di riferimento per tutti gli altri documenti del SGIG.

Le informazioni documentate sono suddivise in:

- ✓ documenti del SGIG a livello di Gruppo;
- ✓ documenti del SGI a livello di Singola Azienda: Eurolink S.r.l., Infordata S.p.A. e Technis Blu S.r.l.;
- ✓ documenti del SGQ rispetto Infordata Education S.r.l..

6 Riesame

Le presenti politiche vengono riesaminate dalle Direzioni regolarmente o in caso di cambiamenti significativi che influenzano il SGIG, al fine di garantire l'idoneità, l'adeguatezza e l'efficacia del SGIG.