POLITICA

Politica Integrata Qualità e Sicurezza delle Informazioni

***PQS Rev:** 00 del 01/06/2023*

	REDATTO	VERIFICATO	APPROVATO
Revisione	data: 01/06/2023	data: 01/06/2023	data: 01/06/2023
00	Consulente	Chiara Mantellini	Fabrizio Fiocchi
Descrizione Modifiche	*Prima emissione*		

PRIMA EMISSIONE

Riferimenti a documenti aziendali:

- nessuno.

Riferimenti esterni:

- Norma ISO 9001:2015 - Sistemi di gestione per la qualità – Requisiti
- Norma ISO/IEC 27001:2013 -Tecnologie informatiche – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- Norma ISO/IEC 27017:2015 - Tecnologie informatiche – Tecniche per la sicurezza - Codice di condotta per i controlli di sicurezza basati sulla ISO/IEC 27002 per servizi cloud
- Norma ISO/IEC 27018:2019 - Tecnologie informatiche – Tecniche per la sicurezza - Codice di condotta per la protezione delle PII (Personally Identifiable Information) nei servizi di public cloud per i cloud provider
- Norma ISO/IEC 27002 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni

Indice

1. INTRODUZIONE

1.1. Premessa

Il Sistema di Gestione Integrato di ESGeo Srl è sviluppato in conformità alle norme seguenti:

- ISO 9001:2015 - Sistema di Gestione per la Qualità (SGQ), che rappresenta un elemento centrale dell'organizzazione e dei processi aziendali, focalizzato alla soddisfazione del Cliente
- ISO/IEC 27001: 2013 - Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), al fine di garantire riservatezza, integrità e disponibilità delle informazioni utilizzate e gestite presso la propria Server Farm
- ISO/IEC 27017:2015 - Codice di condotta per i controlli di sicurezza per servizi cloud basati sulla ISO 27002
- ISO/IEC 27018:2019 - Codice di condotta per la protezione delle PII (Personally Identifiable Information) nei servizi di public cloud per i cloud provider

L'ambito di applicazione delle norme sopra citate è così differenziato:

SCHEMA	CAMPO DI APPLICAZIONE	SETTORE
ISO 9001 ISO/IEC 27001 ed estensioni	Servizi di Cloud computing in modalità SaaS, IaaS e PaaS, gestione del ciclo di sviluppo di prodotti software e relative attività di manutenzione; conduzione di servizi applicativi	**EA33**

Dove il codice EA definisce il Settore di Certificazione:

EA33: Tecnologia dell'informazione.

Il presente documento fornisce un quadro di insieme delle politiche adottate per la realizzazione del Sistema di Gestione Integrato aziendale, con l'intento di promuoverne l'attuazione e la diffusione all'interno dell'azienda e di favorire il raggiungimento degli obiettivi previsti.
A supporto di quanto espresso nel presente documento, è stato elaborato dall'Alta Direzione della Società la politica integrata Qualità e Sicurezza delle informazioni che esprime principi, obiettivi, impegno e leadership, relativamente al sistema di gestione integrato 9001 e 27001.

1.2 Scopo

La presente politica è utilizzata quale strumento per sensibilizzare l'intera organizzazione su principi di qualità, sicurezza delle informazioni aziendali, gestione dei servizi, continuità operativa.

1.3 Area di Applicazione

La presente politica si applica, sotto il governo ed il supporto della Direzione, a tutto il personale aziendale e ai clienti e fornitori coinvolti nel campo di applicazione del Sistema di Gestione Integrato.

1.4 Acronimi e abbreviazioni

Nel documento sono utilizzati i seguenti acronimi:

- **GDPR**: General Data Protection Regulation
- **DVR**: Documento di Valutazione dei Rischi
- **SGCO**: Sistema di Gestione per la Continuità Operativa
- **SGI**: Sistema di Gestione Integrato
- **SGQ**: Sistema di Gestione per la Qualità
- **SGSI**: Sistema di Gestione per la Sicurezza delle Informazioni

2. DESCRIZIONE POLITICA

La presente politica aziendale integrata è stata sviluppata sulla base degli standard internazionali che forniscono i requisiti di Sistemi di Gestione per la Qualità - ISO 9001:2015, per la Sicurezza delle Informazioni - ISO/IEC 27001:2013, ISO/IEC 27107:2015, ISO/IEC 27018:2019,

Tale scelta corrisponde, essenzialmente, alle seguenti esigenze:

- Definire un sistema che consenta di implementare e governare l'insieme delle misure organizzative, fisiche e logiche necessarie a garantire la qualità del servizio, la protezione delle informazioni aziendali ivi compresi i dati personali e garantisca la sicurezza e disponibilità dei servizi offerti, nel rispetto di regole a tutela dell'ambiente e della salute e sicurezza sul lavoro del personale
- individuare e includere i diversi ambiti di cui si compone un sistema di gestione integrato.

Il documento delinea i principi strategici ai quali ENGeo Srl Intende ispirarsi per raggiungere i propri obiettivi. Tali principi possono essere sintetizzati in:

- Focalizzazione sul Cliente
- Leadership
- Partecipazione attiva delle persone
- Approccio per processi
- Miglioramento continuo
- Analisi dei Rischi
- Gestione delle relazioni
- Garanzia di Riservatezza, Integrità e Disponibilità delle Informazioni
- Esercizio dei diritti degli interessati in ambito privacy
- Continuità nel fornire prodotti ed erogare servizi a livelli predefiniti
- Gestione sostenibile dell'ambiente
- Salvaguardia della salute e sicurezza sul lavoro delle risorse umane.

Nel dettaglio i principali processi identificati sono:

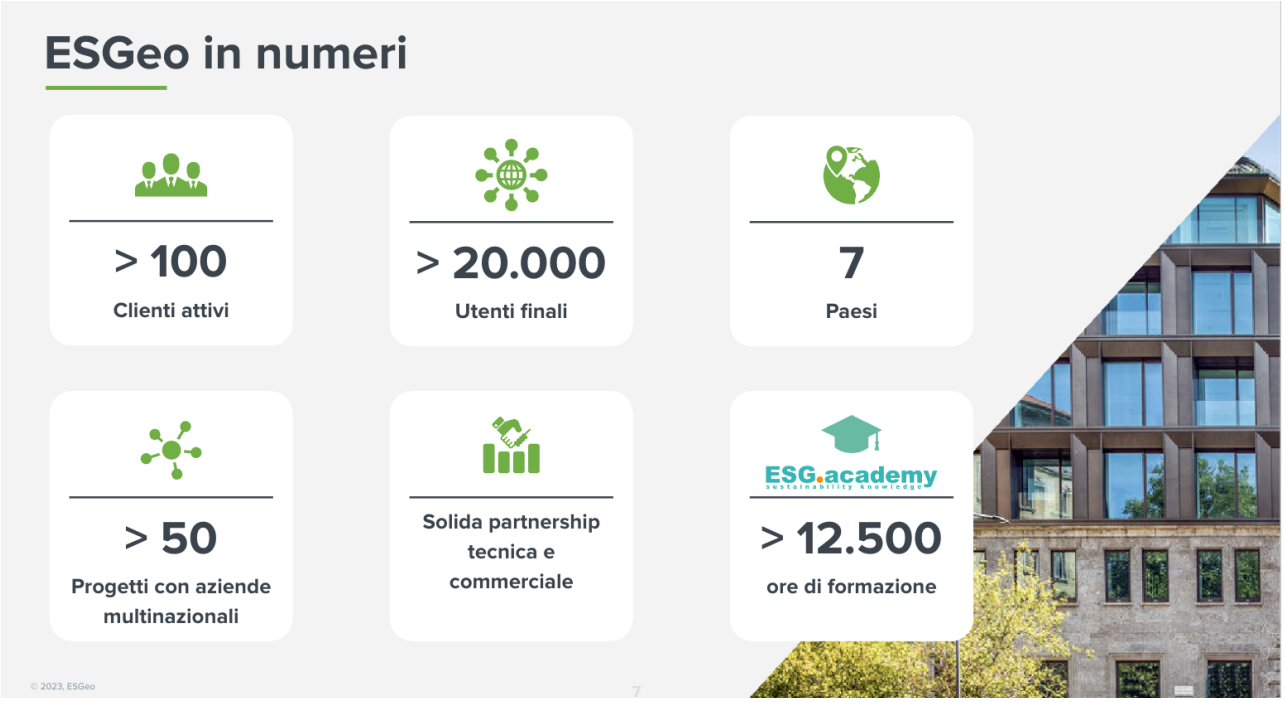
- gestione degli asset
- gestione delle risorse umane, in particolare organizzazione
- gestione della comunicazione
- gestione dei fornitori
- sicurezza fisica ed ambientale
- gestione operativa delle risorse informatiche
- controllo accessi

- acquisizione, sviluppo e manutenzione dei sistemi informativi
- progettazione, sviluppo, controllo, riesame, produzione ed erogazione del prodotto/servizio
- soddisfazione del Cliente
- gestione degli incidenti di sicurezza
- gestione della continuità operativa
- gestione dei servizi erogati
- gestione delle modifiche
- conformità.

2.1 Mission aziendale

Fondata nel 2019 a Milano, ESGeo è una società dedicata alla gestione della data governance degli impatti ESG. Fondata dal gruppo Avvale e il manager Fabrizio Fiocchi, conta oltre 90 clienti prevalentemente multinazionali operanti in diversi settori. Ha uffici in Italia, Spagna, Germania e Stati Uniti.

ESGeo è una società che opera nella consulenza e nella fornitura di soluzioni dedicate alla sostenibilità e supporta le aziende nella gestione dei dati e il reporting di impatti diretti (DNF, Rating Report, Report ESG, Rating ESG, impact investing, etc.) e indiretti (Value chain) riducendo i tempi di implementazione, l'affidabilità delle informazioni e migliorando gli impatti generati.



La piattaforma

Misurare e gestire gli obiettivi non finanziari non è solo un obbligo normativo, ma anche una grande **opportunità per aumentare il valore delle iniziative, ridurre i rischi reputazionali e le controversie legate alla sostenibilità**.

Il software ESGeo è un'applicazione SaaS (Software as a Service) che utilizza la piattaforma Microsoft Azure per erogare il servizio.

ESGeo è certificato dai GRI Standards ed è SASB inside. Garantisce inoltre l'allineamento ai nuovi standard europei (ESRS).

GRI SOFTWARE & TOOLS PARTNER

SASB INSIDE

ESGeo è una soluzione tecnologica integrata per la gestione:

- della raccolta dati qualitativi e quantitativi legati alla sostenibilità (starter kit che contiene i principali KPI previsti dal GRI Standards);
- del calcolo, conversione e consolidamento dei KPI;
- del workflow e monitoraggio degli stessi;
- del reporting dei contenuti collegati alla sostenibilità a supporto della preparazione della Dichiarazione Non Finanziaria o Bilancio di Sostenibilità;
- della tracciabilità dell'intero processo end to end.

ESGeo è la piattaforma principale per la gestione integrata dei dati non finanziari, in cui i KPI vengono raccolti, elaborati, convertiti e aggregati a ogni livello della gerarchia delle unità organizzative, al fine di produrre l'output finale per il rapporto annuale di sostenibilità. Un flusso di lavoro strutturato e un'interfaccia intuitiva consentono di impostare un processo guidato in cui ogni utente ha un ruolo definito ed è in grado di svolgere i propri compiti in un ambiente di facile utilizzo, conforme ai requisiti di audit interni ed esterni.

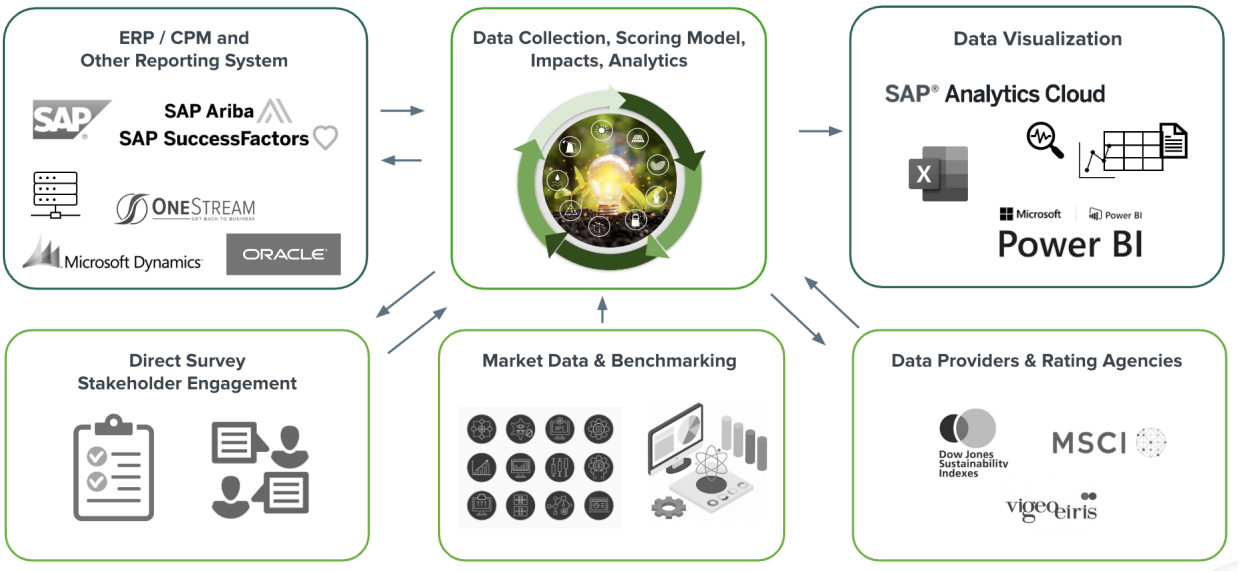
Grazie al know-how maturato in questi anni nel supporto al processo di data collection e rendicontazione in primari gruppi e PMI, siamo in grado di poter offrire al cliente una soluzione che consenta un approccio distintivo e specifico rispetto ai desiderata delineati.

Forniamo quindi un modello di consulenza basato sulla realizzazione di una proposta verticale che consenta di migliorare e semplificare l'intero processo di rendicontazione.

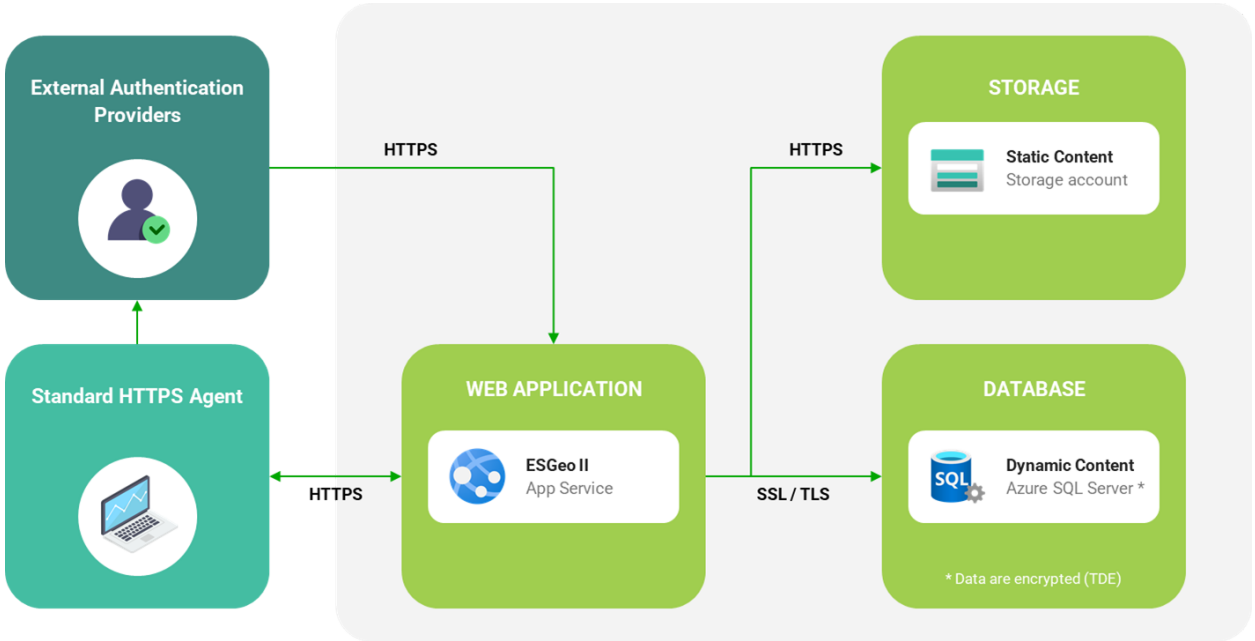
La soluzione proposta, sulla base dei desiderata definiti con il cliente, sarà in grado di integrare future evoluzioni e/o aggiornamenti da GRI standards (o SASB), comprese le direttive emesse dalla Normativa Europea (nuovi principi di rendicontazione European Sustainability Reporting Standards (ESRS) elaborati dall'EFRAG secondo la CSRD); con gli obblighi di adempimenti normativi e con le best practice di ESGeo copre tutte le funzionalità end to end della data collection e Reporting ed è integrabile con le piattaforme aziendali e con gli info provider.

L'architettura di ESGeo è stata pensata per sfruttare al meglio le potenzialità messe a disposizione dalla piattaforma Microsoft Azure ed è, inoltre, dotata di un API Layer per connettersi con diversi applicativi.

ESGeo è integrabile con le principali piattaforme di e-procurement i (SAP, ARIBA, JAGGAER, Ivalua Coupa etc.) e con gli info provider oltreché con gli altri sistemi Legacy dell'azienda cliente. Può raccogliere informazioni da contributori esterni all'azienda (survey stakeholder e fornitori). Può fare l'upload di informazioni da data provider esterni ed è pienamente integrato con la suite office e Power BI per il Dashboarding e il reporting.



L'architettura di ESGeo è stata pensata per sfruttare al meglio le potenzialità messe a disposizione dalla piattaforma Microsoft Azure.

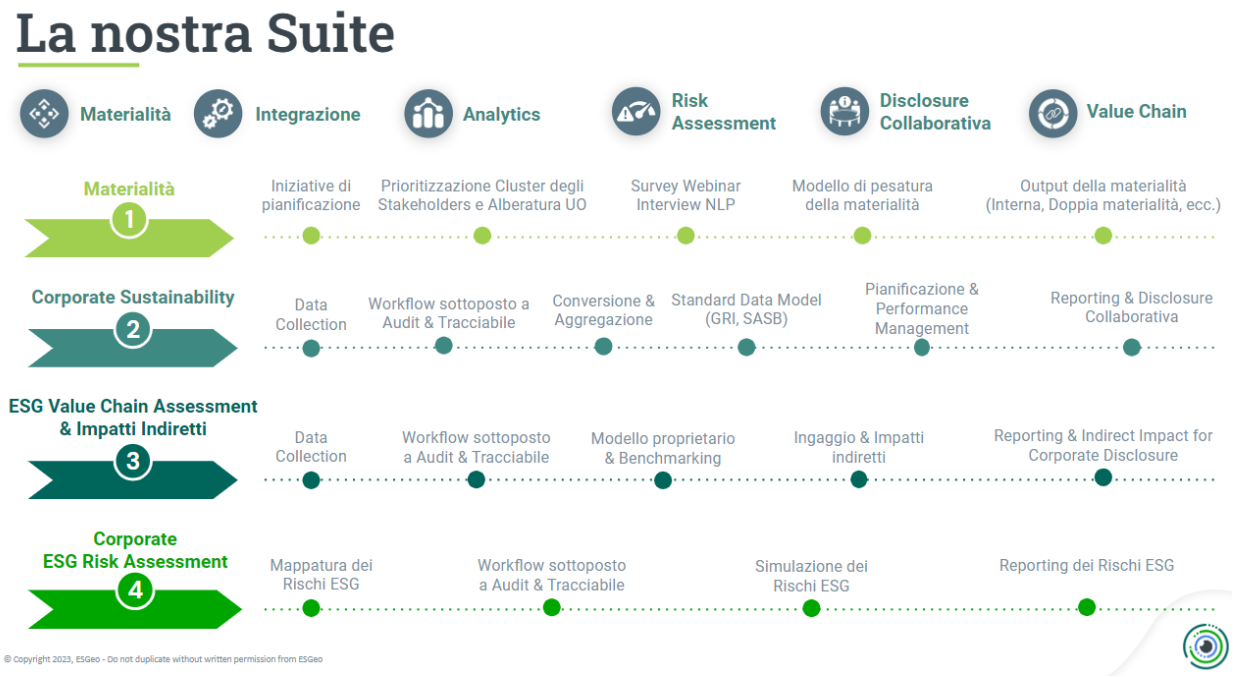


L'obiettivo della nostra proposta è quello di accompagnare il cliente nel processo di gestione e rendicontazione dei dati non finanziari, ovvero di adottare un workflow strutturato, tracciato e ricostruibile per la redazione del bilancio di sostenibilità. Di fatto, dotarsi di uno strumento di Digital Governance per i dati non finanziari.

L'approccio metodologico realizzato assieme ad ESGeo consentirà al Gruppo di raggiungere inoltre anche altre importanti finalità, quali componenti chiave e parti fondamentali di un simile processo di gestione dati:

- Valutazione della materialità per dare priorità alle questioni più importanti per l'organizzazione e i suoi stakeholder e progettare la matrice di materialità.
- Definizione dell'identità ESG per delineare una strategia di sostenibilità allineata alla visione aziendale e stabilire gli obiettivi più appropriati.
- Sviluppo di un modello di punteggio ESG proprietario per misurare le opportunità e i rischi ESG dell'azienda, per misurare la performance ESG aziendale attraverso le filiali e i manager o per misurare gli impatti di entità esterne come investimenti, prestiti o fornitori.
- Trasformare i dati in valore analizzando i risultati aziendali e confrontandoli con quelli dei concorrenti.
- Analisi della catena di fornitura per guidare l'azienda nella progettazione della valutazione della catena di fornitura, dei contributi all'impatto della catena di fornitura (ad esempio, GHG Scope 3) e della mappatura e del punteggio dei fornitori.
- Reporting di sostenibilità per divulgare gli obiettivi ambientali, sociali e di governance e i progressi compiuti per raggiungerli, migliorando la reputazione aziendale, la trasparenza, la fiducia degli stakeholder e riducendo i rischi.

- Strategia di comunicazione per convertire i rischi di comunicazione in opportunità con un quadro di dati completamente verificabili e tracciabili.



2.2 Risorse da salvaguardare

Le risorse che ESGeo Srl si impegna a salvaguardare sono tutte quelle che sottendono ai processi strategici e che sono attentamente elencate nell'asset inventory aziendale. Le categorie principali sono:

- dati/documenti
- asset fisici
- asset logici
- servizi
- personale.

Relativamente all'ambito del delivery di servizi ed in conformità alle norme ISO/IEC 27001:2013, e alle sue estensioni ISO/IEC 27017:2015, ISO/IEC 27018:2019, viene condotta con frequenza annuale un'analisi dei rischi che incombono sugli asset aziendali e sui trattamenti che afferiscono ai dati personali. Tale analisi tiene in considerazione gli obiettivi strategici espressi nella presente

politica, gli incidenti occorsi, i cambiamenti di business e di tecnologia avvenuti nel corso del periodo.

2.3 Obiettivi di ESGeo Srl

I principi base che guidano l'azione di ENGeo Srl Sono:

- ottenere la massima soddisfazione del cliente e delle altre parti interessate, quali, ad esempio, i cittadini, nel rispetto delle loro aspettative ed esigenze, fornendo servizi di elevata qualità
- offrire un adeguato livello di sicurezza dei dati e delle informazioni trattate durante la gestione dei processi di delivery di servizi, identificando, valutando e trattando i rischi ai quali i servizi stessi possono essere soggetti
- garantire la protezione dei dati personali nei trattamenti gestiti sia in qualità di Titolare sia in qualità di Responsabile del Trattamento
- garantire che i propri servizi siano sistematicamente rispondenti agli SLA (Service Level Agreement) concordati con i rispettivi clienti
- assicurare la continuità dei servizi grazie ad una adeguata allocazione di risorse atte a garantire l'identificazione e l'impatto di potenziali perdite, il mantenimento dei piani e delle strategie di ripristino
- predisporre luoghi di lavoro sicuri e salubri, migliorare la salute e sicurezza sul lavoro, eliminare i pericoli e minimizzarne i rischi.

Con la presente politica ESGeo Srl intende formalizzare i seguenti obiettivi generali nell'ambito del sistema di gestione integrato:

- Fornire con regolarità servizi che soddisfino i requisiti del cliente e quelli cogenti e normativi applicabili.
- Facilitare le opportunità per accrescere la soddisfazione del cliente.
- Affrontare rischi ed opportunità associati al contesto e ai propri obiettivi.
- Dimostrare la conformità ai requisiti specificati dal Sistema di Gestione Integrato.
- Preservare al meglio l'immagine dell'azienda quale soggetto affidabile e competente.
- Fornire pieno supporto e commitment al fine di raggiungere la compliance dei requisiti cogenti in maniera di trattamento di dati personali (GDPR).
- Proteggere il proprio patrimonio informativo in modo che:
    - le informazioni siano protette da accessi non autorizzati tramite opportune politiche di accesso basate sui requisiti relativi alla sicurezza e all'attività dell'azienda;

  - le informazioni non vengano divulgate a personale non autorizzato a seguito di azioni deliberate o per incuria;
  - l'integrità delle informazioni sia protetta e salvaguardata da modifiche non autorizzate;
  - le risorse di supporto alle informazioni siano protette adeguatamente.

- Assicurare la protezione dei dati personali adempiendo agli obblighi dettati dal Regolamento Generale sulla Protezione dei Dati (GDPR) e la relativa normativa italiana attraverso:
  - l'elaborazione del registro delle attività di trattamento;
  - la valutazione di impatto sulla protezione dei dati, laddove applicabile;
  - l'applicazione di misure tecniche ed organizzative adeguate intese a garantire la sicurezza dei dati e assicurarne l'accountability e il rispetto dei principi di privacy by design e by default, in modo che i dati siano:
    - trattati in modo lecito, corretto e trasparente
    - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità
    - adeguati, pertinenti e non sovrabbondanti
    - accurati e mantenuti aggiornati
    - non conservati più a lungo del necessario
    - trattati in conformità dei diritti dell'interessato
    - sicuri
    - non trasferiti all'estero senza adeguata protezione.
- Assicurare la continuità del business aziendale affinché le informazioni siano a disposizione degli utenti autorizzati quando ne abbiano necessità tramite:
  - predisposizione di sistemi di backup delle informazioni uniformemente gestito e monitorato;
  - redazione di piani per la gestione del servizio, tra cui piani della continuità, mantenuti costantemente aggiornati e controllati;
  - redazione di piani per la continuità dell'attività aziendale, opportunamente aggiornati, controllati e migliorati, ai fini di assicurare capacità di risposta a eventi disastrosi, resilienza e continuità dei servizi.
- Minimizzare i danni derivanti da attività esterne, interne, accidentali o intenzionali mediante:
  - controlli opportuni per l'accesso alle informazioni o agli asset dell'azienda da parte di terzi;

  - mantenimento della sicurezza dell'informazione e del software scambiato all'interno dell'azienda con qualunque parte esterna;
  - procedure per le necessarie autorizzazioni a portare fuori dall'azienda informazioni critiche, apparati e/o software;
  - procedure per la sicurezza degli apparati all'esterno dell'azienda stabilendo le modalità di assegnazione degli accessi.
- Rispondere e reagire tempestivamente ad eventi che possano ridurre la sicurezza delle informazioni mediante:
  - redazione di procedure per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione, in modo che siano immediatamente individuabili i responsabili e le azioni correttive da intraprendere;
  - comunicazioni tempestive a chi di dovere relativamente a violazioni della sicurezza delle informazioni.
- Rispondere pienamente alle indicazioni della normativa vigente e cogente.
- Aumentare, nella propria organizzazione, il livello di sensibilità e la competenza sui temi di sicurezza attraverso:
  - comunicazioni aggiornate e adeguata formazione per tutto il personale, circa l'attuazione del SGSI;
  - programmi formativi di dettaglio sulla sicurezza delle informazioni per tutto il personale interno e per tutto il personale esterno che opera per periodi prolungati all'interno dell'azienda.
- Fornire opportunità di miglioramento continuo.
- Definire e mantenere sotto controllo, per quanto riguarda l'erogazione di servizi in modalità cloud:
  - le modalità di erogazione del servizio in cloud: IaaS e PaaS;
  - la gestione degli accessi ai servizi erogati in modalità cloud, secondo la Politica degli Accessi Logici di ESGeo Srl;
  - le comunicazioni ai customer in caso di change e agli interessati in caso di data breach, attraverso sistema di trouble ticketing;
  - il ciclo di vita degli account, definito nelle note operative relative ai servizi erogati in modalità cloud;
  - il recepimento nell'analisi del rischio dei rischi aggiuntivi derivanti dall'erogazione di una infrastruttura cloud: l'analisi del rischio ISO/IEC 27001 viene effettuata includendo gli asset relativi ai servizi in cloud;
  - l'applicazione dei requisiti cogenti derivati dal Regolamento Europeo per la Protezione dei Dati Personal (GDPR).

2.4 Leadership e commitment

L'Alta Direzione di ESGEo Srl, ponendo il SGI quale base prioritaria e strategica per il conseguimento degli obiettivi a carattere generale individuati, intende mostrare la propria leadership e il proprio impegno concreto.

Le principali azioni in tal senso sono:

COMMITMENT	MODALITÀ DI ATTUAZIONE
Assicurare che le Politiche e gli obiettivi del SGI siano stabiliti in modo adeguato.	• Definizione della Politica del Sistema di Gestione Integrato • Riesame della Direzione • Azioni di mitigazione dei rischi • Mantenimento di risorse adeguate • Intervento in caso di violazione delle Politiche del Sistema di Gestione Integrato.
Assicurare un'adeguata integrazione dei processi del SGI nei processi di business dell'organizzazione.	• Attività di formazione e consapevolezza • Attribuzione di adeguati ruoli, responsabilità e autorità.
Rendere disponibili adeguate risorse per il SGI.	• Azioni di mitigazione dei rischi • Piano di miglioramento del SGI
Comunicare l'importanza dell'efficacia del SGI e del conformarsi ai relativi requisiti.	• Attività di formazione e consapevolezza.
Assicurare che il SGI raggiunga gli obiettivi stabiliti.	• Monitoraggio, misurazione e analisi delle azioni di mitigazione dei rischi.
Dirigere e supportare il personale nel contribuire all'efficacia del SGI.	• Attività di formazione e consapevolezza.
Promuovere il miglioramento continuo.	• Attività di formazione e consapevolezza • Piano di miglioramento del SGI.
Supportare i responsabili di	• Riunioni periodiche di pianificazione e

processo nel consolidamento della leadership nelle attività di loro pertinenza.	comunicazione risultati.
Assicurare che il SGI promuova e persegua la completa responsabilizzazione (accountability).	• Rispetto dei requisiti di legge, dei regolamenti, delle direttive (locali, nazionali e comunitarie) applicabili alla realtà dell'azienda, nel rispetto di tutte le parti interessate e delle esigenze dalle stesse espresse durante l'erogazione del servizio • Garanzia di efficacia ed efficienza dei processi aziendali • Disponibilità del presente documento a tutte le parti interessate, tramite adeguati canali di comunicazione al proprio interno e verso l'esterno • Monitoraggio e miglioramento costante dei propri Sistemi di Gestione, definendo obiettivi per il miglioramento e verificandone il raggiungimento e dandone opportuna comunicazione a tutto il personale • Introduzione e costante aggiornamento delle • procedure di gestione e sorveglianza per il costante controllo dell'incolumità del personale, dell'ambiente e delle prestazioni energetiche, al fine di programmare opportuni interventi nel caso si riscontrino situazioni non conformi, anomalie o emergenze • Potenziamento dell'attività di informazione e formazione di tutti gli operatori, garantendo lo sviluppo professionale degli stessi in quanto risorsa strategica, rendendoli consapevoli dei loro obblighi individuali, dell'importanza di ogni loro azione per il raggiungimento dei risultati attesi e della loro responsabilità in materia di ambiente, responsabilità sociale, salute e sicurezza sui luoghi di lavoro • Considerazione dei Clienti quali elemento fondamentale del proprio successo, lavorando per la loro soddisfazione anche riguardo alle regole di Responsabilità Sociale • Considerazione dei propri fornitori come partner, non solo per la realizzazione delle attività ma

	anche per quanto riguarda la Responsabilità Sociale • Identificazione di rischi, opportunità e pericoli derivanti dallo svolgimento delle attività, tramite valutazione preventiva di rischi per il personale per le attività in essere e per ogni nuova attività e/o processo, in modo da adottare soluzioni in grado di prevenire infortuni, patologie professionali, impatti sull'ambiente e sprechi energetici, e minimizzare, per quanto possibile, l'accadimento e l'estensione di tali eventi • Conduzione periodica di audit interni; analisi e monitoraggio di eventuali non conformità.

2.5 Analisi dei rischi

La Direzione ha istituito ed attua un approccio basato sulla valutazione quantitativa e qualitativa dei rischi associati alle risorse esistenti in azienda, ai processi e agli obiettivi definiti nel sistema, ai trattamenti dei dati personali. Tale metodo consente di determinare valori oggettivi che permettono di definire le relative contromisure che devono essere adottate per abbattere e rendere accettabile il valore del rischio residuo associato al bene. In tal senso vengono adottati strumenti informatici e metodi deterministici che permettono, oltre che di implementare e gestire l'inventario degli asset aziendali, il registro dei trattamenti dei dati personali, misurare l'efficacia dell'applicazione delle azioni e soprattutto la replicabilità della valutazione, in ottica di garantire il processo di miglioramento. Inoltre, l'analisi dei rischi costituisce strumento fondamentale a supporto delle decisioni dell'organizzazione, al fine di evitare rischi e cogliere opportunità.
Le analisi dei rischi e i relativi piani di trattamento sono presentati e valutati ad ogni riesame della Direzione al fine di individuare opportunità di miglioramento e definire misure di sicurezza. Tali misure di sicurezza hanno lo scopo di "contrastare", "prevenire", "dissuadere", "rilevare", "attenuare", "ripristinare" o "correggere" le minacce che possono incombere sui sistemi informativi aziendali. Esse dovranno essere attuate secondo le modalità descritte all'interno di specifiche procedure operative e/o istruzioni operative.

3. RESPONSABILITÀ E VIOLAZIONI

3.1 Responsabilità

La presente politica è stata formulata dal Consulente in collaborazione con Responsabile del SGQ e del SGI, che, su incarico della Direzione, estende la responsabilità su tutti i sistemi di gestione.
Essa verrà riesaminata almeno annualmente ad ogni riesame della Direzione e comunque al verificarsi di cambiamenti significativi.

I responsabili dell'attuazione della presente politica sono:

- La Direzione ESGeo Srl, che stabilisce i criteri di accettazione e i livelli di accettabilità del rischio e fornisce le risorse necessarie per garantire la corretta applicazione dei processi del Sistema di Gestione Integrato, assicura lo svolgimento di audit interni e garantisce il pieno supporto nell'attuazione della presente politica, affidando alle diverse funzioni compiti di implementazione, gestione e monitoraggio dell'efficacia ed efficienza del sistema, assegna opportuni ruoli e responsabilità per la gestione per la qualità, la gestione per la sicurezza dell'informazione, la gestione del servizio e per la continuità operativa.
- Il Titolare per il Trattamento dei dati personali, nella figura dell'Amministratore Unico, che ha la responsabilità di qualsiasi trattamento di dati personali che effettui direttamente o che altri effettuino per suo conto. In particolare mette in atto misure adeguate ed efficaci, così da essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, compresa l'efficacia delle misure, che tengono 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.
- Il Responsabile del SGI, che facilita l'attuazione della presente politica attraverso norme e procedure appropriate.
- Tutto il personale di ESGeo Srl, a cui sono assegnati precisi ruoli e responsabilità. Esso deve avere un'adeguata competenza per svolgere i compiti richiesti, pertanto deve essere informato e formato adeguatamente riguardo agli obiettivi dell'azienda in tema di qualità, sicurezza delle informazioni, protezione dei dati personali, gestione dei servizi, continuità operativa, salute e sicurezza sul lavoro, gestione ambientale. Sono definite e mantenute registrazioni sull'istruzione, formazione, abilità, esperienze e qualifiche. Tutto il personale ha la responsabilità di reagire tempestivamente agli incidenti contro la sicurezza e/o non conformità del prodotto/servizio e a segnalare alla Direzione qualsiasi punto debole individuato nel sistema.
- Clienti e Fornitori coinvolti nella gestione dei prodotti/servizi implementati, che rientrano nel perimetro di applicazione del Sistema di Gestione Integrato. Essi sono tenuti al rispetto della Politica Integrata di ESGeo Srl.

3.2 Violazioni

L'Alta Direzione è coinvolta in prima persona nel rispetto e nell'attuazione di questi principi e si impegna ad assicurare che la presente politica sia compresa, condivisa, implementata e attuata da tutti i propri dipendenti e collaboratori ed allo stesso tempo si impegna a condividerla con tutti gli stakeholder.
Ritenendo di fondamentale importanza la realizzazione degli obiettivi fissati, il Sistema di Gestione Integrato è costantemente monitorato e si dà atto che ogni azione non conforme alla presente politica aziendale verrà esaminata e potrà dare origine all'adozione di provvedimenti in coerenza con le disposizioni di legge e con i previsti regimi contrattuali applicabili caso per caso.

For any further information or additional clarification, please contact

helpdesk@esgeo.eu