SISTEMA DI GESTIONE INTEGRATO

Redatto:	F. Tortorelli	20.08.2024
Verificato:	F. Tortorelli	30.08.2024
Approvato:	E. Castanini	03.09.2024
Versione:	11	
Distribuito:	Siti Intranet e Internet Liguria Digitale S.p.A.	

DATI DI CONTROLLO DEL DOCUMENTO

Storia del documento				
versione	data	capitolo/paragrafo	modifica apportata	motivo modifica
01	19.07.2019	---	nessuna	---
02	08.10.2019	tutti	inserimento riferimenti a norme 20000 e 22301	integrazione con norme 20000 e 22301
03	18.10.2019	2.4	inclusi i punti richiesti dalla norma ISO/IEC 27001 per i Cloud service provider	Bureau Veritas Italia S.p.A. - Rapporto di audit - Verifica Iniziale ISO 27001:2013
04	01.09.2020	tutti	inserimento riferimenti a norme 27701,14001,45001	estensione a 27701 integrazione con 14001, 45001
05	11.10.2021	1.1. 2.2. ovunque citati	ampliamento ambito aggiornata mappa dei processi aggiornamento riferimenti norme 27018 e 22301 alla edizione 2019	estensione 9001, 27001, 27701, 14001 e 45001 all'intera azienda adeguamento alle edizioni correnti
06	01.09.2022	tutti	inserimento riferimenti a norma 50001	certificazione 50001
07	21.09.2022	2.4.	inserimento specificazioni customer cloud	estensione 27017 - customer cloud
08	13.03.2023	1.1. 2.4.	ampliamento ambiti e precisazioni inserita modalità cloud provider SaaS aggiornamento codici EA/IAF	estensione ambito ai servizi cloud SaaS (per 9001, 27001, 27017, 27018, 27701, 20000-1, 22301) inserimento codice 37 per la 9001

08	13.03.2023	1.4. 2.3.	inseriti acronimi EA, IAF, EGE, WTC redazione diagnosi energetica da 1 a 4 anni	precisazioni adeguamento alla normativa vigente
09	14.07.2023	1.1.; 1.2.; 1.4.; 2.; 2.4.; 3.1.	inseriti riferimenti alla parità di genere (UNI/PdR 125:2022 – Linee guida sul sistema di gestione per la parità di genere)	Certificazione UNI/PdR 125:2022
10	08.08.2023	1.1.	inserito UNI/PdR 125 nella colonna *Schema* della tabella "Campo di Applicazione"	Certification s.r.l. – PdR 125 - Rapporto di audit Stage 1 - Rilievo azione 2023-08
11	03.09.2024	Riferimenti esterni 1.1. 2., 2.3. 1.4.	aggiornamento riferimenti norma 27001 edizione 2022 inserimento riferimenti norme 27035-1 e 27035-2 aggiornamento riferimenti norma 45001 edizione 2023 inserimento riferimenti schema CSA STAR – Level 2 acronimi relativi	Transizione a nuova norma ISO/IEC 27001:2022 Estensione a ISO/IEC 27035-1:2023 ISO/IEC 27035-2:2023 adeguamento all'edizione corrente di UNI EN ISO 45001 Certificazione CSA STAR – Level 2
		2.4. 1.4.	introduzione valutazione del cambiamento climatico acronimi relativi	Recepimento dell'addendum delle ISO: 9001, 14001 e 45001/Amd 1:2024, (§ 4.1 e § 4.2)
		1.2.; 2.; 2.4.; 3.1.	esplicitati riferimenti a concetti di inclusione/non discriminazione	prossima redazione del bilancio di sostenibilità

Riferimenti a documenti aziendali:

- nessuno.

Riferimenti esterni:

- Norma ISO 9001:2015 - Sistemi di gestione per la qualità – Requisiti
- ISO 9001:2015/Modifica 1:2024 - Sistemi di gestione per la qualità – Requisiti – Emendamento 1:2024 – Cambiamenti nell'azione per il clima
- Norma ISO/IEC 27001:2022 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - 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 27701:2019 - Tecnologie di sicurezza – Estensione alla ISO/IEC 27001 e ISO/IEC 27002 per la gestione di informativa sulla privacy - Requisiti e linee guida
- Norma ISO/IEC 27035-1:2023 – Information technology — Information security incident management — Part 1: Principles and process
- Norma ISO/IEC 27035-2:2023 - Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- Norma ISO/IEC 20000-1:2018 – Tecnologie informatiche - Gestione del servizio – Parte1: Requisiti per un sistema di gestione del servizio
- Norma ISO 22301:2019 - Sicurezza e resilienza - Sistemi di gestione per la continuità operativa - Requisiti
- Norma ISO 14001:2015 – Sistemi di gestione ambientale – Requisiti e guida per l'uso
- ISO 14001:2015/Modifica 1:2024 - Sistemi di gestione ambientale – Requisiti e guida per l'uso – Emendamento 1:2024 – Cambiamenti nell'azione per il clima
- Norma UNI EN ISO 45001:2023 – Sistemi di gestione per la salute e sicurezza sul lavoro – Requisiti e guida per l'uso
- ISO 45001:2018/Modifica 1:2024 - Sistemi di gestione per la salute e sicurezza sul lavoro – Requisiti e guida per l'uso – Emendamento 1:2024 – Cambiamenti nell'azione per il clima
- Norma UNI CEI EN ISO 50001:2018 - Sistemi di gestione dell'energia - Requisiti e linee guida per l'uso
- Prassi di riferimento UNI/PdR 125:2022 – Linee guida sul sistema di gestione per la parità di genere
- CSA STAR – Level 2 - Schema di certificazione della sicurezza dei servizi cloud.

INDICE

1. INTRODUZIONE

1.1. Premessa

Il Sistema di Gestione Integrato di Liguria Digitale 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: 2022 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni
- 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
- ISO/IEC 27701:2019 - Tecnologie di sicurezza – Estensione alla ISO/IEC 27001 e ISO/IEC 27002 per la gestione di informativa sulla privacy - Requisiti e linee guida
- ISO/IEC 27035-1:2023 – Information technology — Information security incident management — Part 1: Principles and process
- ISO/IEC 27035-2:2023 - Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 20000-1:2018 - Sistema di Gestione del Servizio (SGS), al fine di garantire le modalità di erogazione dei servizi e rispondenza dei servizi erogati con quanto stabilito contrattualmente
- ISO 22301:2019 - Sistema di Gestione per la Continuità Operativa (SGCO), finalizzato alla protezione, alla riduzione della possibilità di accadimento, alla preparazione, alla risposta ed al recupero a seguito di eventi destabilizzanti quando si manifestano
- ISO 14001:2015 – Sistema di Gestione Ambientale (SGA), al fine di gestire le responsabilità ambientali dell'azienda in modo sistematico, contribuendo al pilastro ambientale della sostenibilità
- ISO 45001:2023 – Sistema di Gestione per la Salute e Sicurezza sul Lavoro (SGSSL), al fine di predisporre luoghi di lavoro sicuri e salubri, migliorare la salute e sicurezza sul lavoro, eliminare i pericoli e minimizzarne i rischi
- UNI CEI EN 50001:2018 - Sistema di Gestione dell'Energia (SGE), al fine di stabilire, attuare, mantenere e migliorare un sistema di gestione dell'energia.

Il Sistema di Gestione Integrato di Liguria Digitale è sviluppato inoltre in conformità alla Prassi di riferimento seguente:

- UNI/PdR 125:2022 - Linee guida sul sistema di gestione per la parità di genere.

Il Sistema di Gestione Integrato di Liguria Digitale, infine, tramite l'utilizzo della Cloud Control Matrix - CCM, integra il sistema di gestione ISO 27001 con specifici controlli sulla sicurezza dei servizi cloud (197 controlli suddivisi in 17 Domini), recependo quindi i requisiti dettati dallo schema di certificazione:

- CSA STAR – Level 2 - Schema di certificazione della sicurezza dei servizi cloud.

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

Schema	***Campo Applicazione***	***Settore***
ISO 9001 ***UNI/PdR 125***	Gestione di sistemi in Housing, Hosting e Outsourcing, servizi di Cloud computing in modalità IaaS, PaaS e SaaS, conduzione Server Farm, inclusi i servizi NOC (Networking Operation Center) e SOC (Security Operation Center) gestione del ciclo di sviluppo di prodotti software e relative attività di manutenzione; conduzione di servizi applicativi; servizi di assistenza utente e gestione delle postazioni di lavoro; servizi di supporto in ambito privacy; gestione di prodotti, eventi e servizi di comunicazione; digital high tech academy.	***EA/IAF33*** ***EA/IAF37***
ISO/IEC 27001 ed estensioni 27017, 27018, 27701, 27035 (-1 e -2) e CSA STAR–Level2	Gestione di sistemi in Housing, Hosting e Outsourcing, servizi di Cloud computing in modalità IaaS, PaaS e SaaS, conduzione Server Farm, inclusi i servizi NOC (Networking Operation Center) e SOC (Security Operation Center) gestione del ciclo di sviluppo di prodotti software e relative attività di manutenzione; conduzione di servizi applicativi; servizi di assistenza utente e gestione delle postazioni di lavoro; servizi di supporto in ambito privacy; gestione di prodotti, eventi e servizi di comunicazione; digital high tech academy e relativa gestione delle informazioni personali, in qualità di Titolare del trattamento e Responsabile del trattamento.	***EA/IAF33***
ISO/IEC 20000-1	Gestione di sistemi in Housing, Hosting e Outsourcing, servizi di Cloud computing in modalità IaaS, PaaS e SaaS, conduzione Server Farm, inclusi i servizi NOC (Networking Operation Center) e SOC (Security Operation Center).	***EA/IAF33***

ISO 22301	Gestione di sistemi in Housing, Hosting e Outsourcing, servizi di Cloud computing in modalità IaaS, PaaS e SaaS, conduzione Server Farm.	***EA/IAF33***
ISO 14001 ***ISO 45001***	Gestione di sistemi in Housing, Hosting e Outsourcing, servizi di Cloud computing in modalità IaaS e PaaS, conduzione Server Farm, inclusi i servizi NOC (Networking Operation Center) e SOC (Security Operation Center) gestione del ciclo di sviluppo di prodotti software e relative attività di manutenzione; conduzione di servizi applicativi; servizi di assistenza utente e gestione delle postazioni di lavoro; servizi di supporto in ambito privacy; gestione di prodotti, eventi e servizi di comunicazione; digital high tech academy e relativa gestione delle informazioni personali, in qualità di Titolare del trattamento e Responsabile del trattamento.	***EA/IAF33***
UNI CEI EN ISO 50001 *(solo WTC)*	Gestione di sistemi in Housing, Hosting e Outsourcing, servizi di Cloud computing in modalità IaaS e PaaS, conduzione Server Farm.	***EA/IAF33***

Dove i codici EA/IAF definiscono il Settore di Certificazione:

EA/IAF33: Tecnologia dell'informazione

EA/IAF37: Istruzione.

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, nel 2019 era stato ideato e realizzato da Liguria Digitale un video, pubblicato sia sulla intranet aziendale, sia sul sito internet di Liguria Digitale, in cui l'Alta Direzione della Società esprime principi, obiettivi, impegno e leadership, relativamente al nucleo certificativo originario e rispetto al sistema di gestione integrato tra le norme 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, protezione dei dati personali, gestione dei servizi, continuità operativa, salute e sicurezza sul lavoro, parità di genere e inclusione, gestione ambientale e dell'energia.

1.3. Area di applicazione

La presente politica si applica, sotto il governo e 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:

- CEI: Comitato Elettrotecnico Italiano
- CEN: Comité Européen de Normalisation
- CCM: Cloud Control Matrix
- CSA: Cloud Security Alliance
- DVR: Documento di Valutazione dei Rischi
- E3P: European Energy Efficiency Platform
- EA: European co-operation for Accreditation
- EGE: Esperto in Gestione dell'Energia
- EN: European Normalization
- IAF: International Accreditation Forum
- IEC: International Electrotechnical Commission
- GDPR: General Data Protection Regulation
- ICT: Information and Communication Technologies
- ISO: International Organization for Standardization
- LCA: Life Cycle Assessment
- PdR: Prassi di Riferimento
- SGA Sistema di Gestione Ambientale
- SGCO: Sistema di Gestione per la Continuità Operativa
- SGE: Sistema di Gestione dell'Energia
- SGI: Sistema di Gestione Integrato
- SGQ: Sistema di Gestione per la Qualità
- SGS: Sistema di Gestione del Servizio
- SGSI: Sistema di Gestione per la Sicurezza delle Informazioni
- SGSSL: Sistemi di Gestione per la Salute e Sicurezza sul Lavoro
- STAR: Security, Trust, Assurance and Risk
- UNI: Ente Nazionale Italiano di Unificazione
- WTC: World Trade Center.

2. DESCRIZIONE POLITICA

La presente politica aziendale integrata è stata sviluppata sulla base degli standard internazionali che forniscono i requisiti di Sistemi di Gestione seguenti:

- per la Qualità – ISO 9001:2015
- per la Sicurezza delle Informazioni – ISO/IEC 27001:2022, con estensione a ISO/IEC 27107:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, ISO/IEC 27035-1, ISO/IEC 27035-2 e CSA STAR – Level 2
- del Servizio - ISO/IEC 20000-1:2018
- per la Continuità Operativa – ISO 22301:2019
- Ambientale – ISO 14001:2015
- per la Salute e Sicurezza sul Lavoro – ISO 45001:2023
- dell'Energia - UNI CEI EN ISO 50001:2018
- per la Parità di Genere – UNI/PdR 125:2022.

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, anche in modalità cloud, nel rispetto di regole a tutela dell'ambiente e volte ad un miglioramento continuo della prestazione energetica, della salute e sicurezza sul lavoro del personale, della parità di genere e dell'eliminazione di ogni discriminazione
- individuare e includere i diversi ambiti di cui si compone un sistema di gestione integrato.

Il documento delinea i principi strategici ai quali Liguria Digitale 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
- Miglioramento della prestazione energetica
- Salvaguardia della salute e sicurezza sul lavoro delle risorse umane
- Rispetto delle politiche per la parità di genere e di inclusione.

Nel dettaglio i principali processi identificati sono:

- gestione degli asset
- gestione delle risorse umane, in particolare organizzazione
- gestione della comunicazione
- gestione dei fornitori
- gestione operativa delle risorse informatiche
- acquisizione, sviluppo e manutenzione dei sistemi informativi
- progettazione, sviluppo, controllo, riesame, produzione ed erogazione del prodotto/servizio
- soddisfazione del Cliente
- gestione degli incidenti e dei problemi
- gestione della continuità operativa
- gestione dei servizi erogati
- gestione delle modifiche
- conformità.

2.1. Mission aziendale

Liguria Digitale, già Datasiel S.p.A. costituita ai sensi della L.R. 9 aprile 1985, n. 17, è oggi una Società per Azioni strutturata al servizio della Regione Liguria e degli Enti Soci che esercitano congiuntamente sulla stessa, secondo il modello del "in house providing" stabilito dall'ordinamento interno e dall'Unione Europea, il controllo analogo a quello esercitato sulle proprie strutture organizzative.

I soci di Liguria Digitale, oltre a Regione Liguria che ne detiene la maggioranza azionaria, sono consultabili sul sito istituzionale dell'azienda.

Liguria Digitale svolge per i Soci le attività previste dalla legge e dallo Statuto, secondo le modalità stabilite dal Disciplinare Quadro e dai Patti Parasociali.

La Società è quindi vincolata a realizzare oltre l'80% del proprio fatturato nei confronti e nell'interesse della Regione Liguria, degli Enti Soci e dei loro organismi ausiliari, per i quali opera "al costo".

Quale organismo partecipato dalla Regione Liguria e dagli Enti pubblici Soci, ha lo scopo di perseguire il miglioramento qualitativo nella gestione pubblica mediante

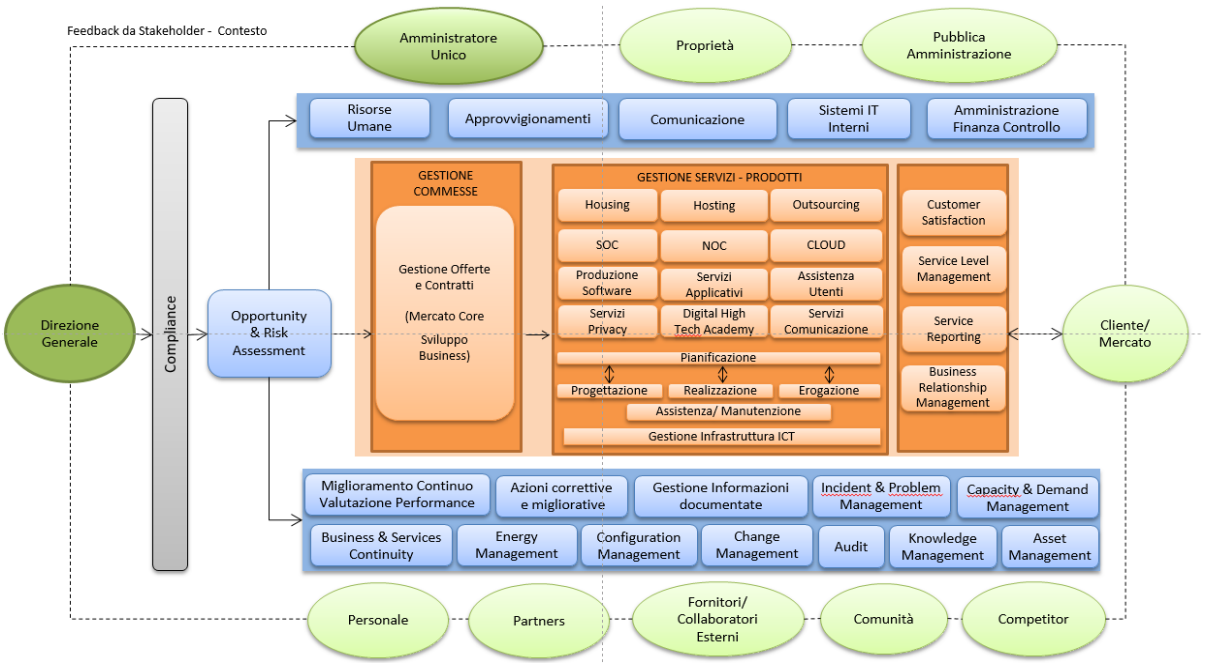
la realizzazione e la messa a disposizione degli operatori pubblici di un sistema integrato di servizi informativi ed informatici e la diffusione di una cultura dell'informazione quale fonte di sviluppo sociale e tecnologico.

La Società svolge inoltre compiti di supporto alla programmazione, assistenza tecnica e consulenza per lo sviluppo della società dell'informazione in Liguria e sulle soluzioni ICT per il sistema pubblico ligure, nonché di promozione dell'innovazione ICT sul territorio anche attraverso iniziative interregionali, nazionali ed europee attuate dalla Regione Liguria e dagli Enti Soci.

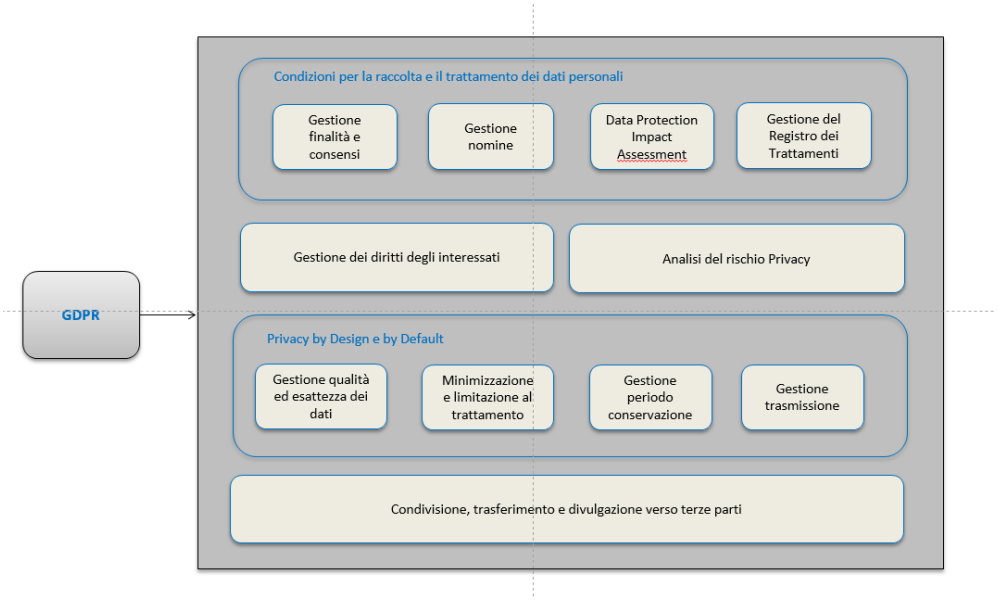
Obiettivo primario di Liguria Digitale, come realtà presente nel contesto istituzionale, economico e sociale del territorio ligure, è la creazione di valore per i Soci, i cittadini, le imprese e i turisti nel più rigoroso rispetto dei principi di onestà, professionalità, integrità morale, nonché correttezza e trasparenza nei rapporti, anche attraverso i comportamenti dei dipendenti e dei collaboratori esterni.

2.2. Processi strategici

I processi strategici per Liguria Digitale, rilevanti per l'ambito del Sistema di Gestione Integrato, sono schematizzati nella figura seguente:



Nell'ambito della Compliance, i processi afferenti alla Privacy, regolati dal GDPR:



2.3. Risorse da salvaguardare

Le risorse che Liguria Digitale 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
- prodotti/servizi
- personale.

Relativamente all'ambito del delivery di servizi ed in conformità alle norme ISO/IEC 27001:2022, e alle sue estensioni ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, ISO/IEC 27035-1, ISO/IEC 27035-2 e CSA STAR – Level 2, alla ISO/IEC 20000-1:2018, alla ISO 22301:2019 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.

Relativamente alla salute e sicurezza sul lavoro, ed in conformità alla norma ISO 45001:2023, almeno annualmente viene rivisto il DVR - Documento di Valutazione dei Rischi aziendale e per la ISO 14001:2015 l'analisi dei rischi ambientali che aiuta ad identificare ed affrontare eventuali situazioni di emergenza ambientale, mentre relativamente alla UNI CEI EN ISO 50001:2018 viene redatta ogni quattro anni, da un professionista specializzato, EGE - Esperto in Gestione dell'Energia, la Diagnosi Energetica del Centro di Elaborazione Dati al WTC.

2.4. Obiettivi di Liguria Digitale

I principi base che guidano l'azione di Liguria Digitale 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 prodotti e 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, anche quelli erogati in modalità cloud, 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 prodotti e 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
- perseguire con approccio sistematico il miglioramento continuo della propria prestazione energetica
- garantire che le proprie attività di business non arrechino danno significativo all'ambiente, tramite una sistematica gestione responsabile
- considerare il cambiamento climatico correlato alle proprie attività e agli obiettivi strategici, garantendo resilienza e adattabilità alle sfide ambientali.

Per mantenere e migliorare tali livelli qualitativi e di sicurezza Liguria Digitale affianca costantemente gli Enti soci, al fine di rendere più efficienti i loro processi interni e di governo dell'amministrazione pubblica e di permettere loro di offrire servizi innovativi a cittadini e imprese.

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

- Fornire con regolarità prodotti e 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, inclusi software e risorse infrastrutturali fruite in modalità cloud;
  - 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 provider:
  - le modalità di erogazione del servizio in cloud: IaaS, PaaS e SaaS;
  - la gestione degli accessi ai servizi erogati in modalità cloud, secondo la Politica degli Accessi Logici di Liguria Digitale;
  - 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 Personali (GDPR).

- Mantenere sotto controllo, per quanto riguarda la fruizione di servizi in modalità cloud customer:
  - le modalità di conservazione e accesso alle informazioni nell'ambiente cloud da parte del cloud service provider;
  - le modalità di manutenzione degli asset di Liguria Digitale siti in cloud da parte del cloud service provider;
  - le modalità di virtualizzazione dei processi in esecuzione in ambienti multi-tenant in cloud;
  - gli utenti che fruiscono i 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 del provider di servizi cloud e i paesi in cui il provider può conservare i dati di Liguria Digitale, anche temporaneamente;
  - gli asset siti in cloud includendoli nell'analisi del rischio ISO/IEC 27001 di Liguria Digitale.
- Assicurare la sicurezza e la salute sul lavoro, anche nel rispetto della parità di genere e di non discriminazione alcuna, e la sicurezza ambientale, mediante un complesso di misure che mirano a garantire un ambiente di lavoro sicuro e salubre per le persone che vi operano, per le apparecchiature utilizzate e per l'ambiente circostante, prevenendo l'inquinamento, riducendo l'entità dei rifiuti, il consumo di energia e dei materiali, in particolare efficientando le prestazioni energetiche.
- Garantire che il Sistema di Gestione Integrato sia resiliente e adattabile alle sfide ambientali.

2.5. Leadership e commitment

L'Alta Direzione di Liguria Digitale, 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 processo nel consolidamento della leadership nelle attività di loro pertinenza.	• Riunioni periodiche di pianificazione e 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

COMMITMENT	MODALITÀ DI ATTUAZIONE
	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, consumo energia • 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

COMMITMENT	MODALITÀ DI ATTUAZIONE
	minimizzare, per quanto possibile, l'accadimento e l'estensione di tali eventi • Conduzione periodica di audit interni; analisi e monitoraggio di eventuali non conformità.
Assicurare che il SGI monitori che le attività dell'azienda non arrechino danno all'ambiente.	• Monitoraggio della catena di fornitura e monitoraggio del LCA, ad es. tramite audit di seconda parte • Mantenimento iscrizione a Piattaforma E3P.

2.6. Analisi dei rischi

La Direzione ha istituito e 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, al DVR, ecc. 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, il DVR, gli impatti ambientali e l'efficienza energetica, di 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 e sulle risorse umane. 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 Responsabile 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 di Liguria Digitale, 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 e per la protezione dei dati personali, la gestione del servizio e per la continuità operativa, la gestione per la salute e sicurezza sul lavoro e per la parità di genere e di non discriminazione, la gestione dell'ambiente e dell'energia.
- 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 Liguria Digitale, 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, parità di genere ed inclusività, gestione ambientale, gestione dell'energia. 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 Liguria Digitale.

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.