Manuale della Qualità e della Sicurezza delle Informazioni di

PuntoZero S.c.a r.l.

RISERVATO: NO

Data:	21/03/2022	**Compilato:**	L. Trappetti
Data:	05/04/2022	**Rivisto:**	G. Bizzarri
Data:	09/05/2022	**Approvato:**	G. Bizzarri
		Distribuzione:	Tutto il personale di PuntoZero S.c.a r.l

INDICE

GENERALITA'

Oggetto:

Il presente manuale costituisce il documento di livello più elevato della documentazione del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni di PUNTOZERO S.c. a r.l.; contiene la Politica e gli obiettivi per la Qualità e la Sicurezza delle informazioni e la descrizione dei processi aziendali certificati

Scopo del documento:

Scopo del documento è descrivere il SGQ adottato in Azienda e rispondere, in particolare, alle seguenti esigenze:

- Descrivere in maniera strutturata e standardizzata i processi che sono alla base delle "fornitura" dei prodotti/servizi offerti dall'organizzazione;
- Fornire informazioni necessarie a comprendere ed applicare, a tutti i livelli, i principi del SGI nonché ad individuare la risposta data dall'azienda ai requisiti richiesti dalla norma ISO 9001:2015 e ISO 27001:2013 (estesa con i controlli delle norme ISO 27017 e ISO 27018) al fine garantire ai clienti dei servizi di PUNTOZERO (inclusi quelli erogati in modalità cloud), che i dati conservati, in particolar modo i dati personali, siano sicuri e protetti;
- Costituire il riferimento per l'attuazione del SGQ.

Campo di applicazione:

È' indirizzato a tutto il personale che coordina, esegue e verifica le attività connesse con il ciclo di vita dei servizi che PUNTOZERO S.c.a r.l. fornisce ai propri soci.

Riferimenti a documenti aziendali:

Tutte le procedure del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni.

Riferimenti normativi

Ai fini del presente documento, si applicano i termini e le definizioni di cui alle norme UNI EN ISO 9001:2015, ISO/IEC 27001:2013, ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

Sono altresì considerate rilevanti ai fini della corretta implementazione:

- Normativa sulla protezione dei dati personali (Regolamento UE 2016/679 - GDPR)
- Codice Amministrazione Digitale (CAD)

Glossario, abbreviazioni e acronimiò

- "SGQ": Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni
- "Manuale processi": contiene lo schema dei processi di PUNTOZERO, e dei relativi rischi associati, ed è reperibile in formato digitale nel Sistema documentale aziendale (https://drive.google.com/drive/folders/1Fpn530FEpQo4oyzqk57KIAJsTym4h304?usp=sharing)
- "Dizionario profili di competenza": contiene il dizionario dei profili di competenza necessari per lo svolgimento dei processi di PUNTOZERO; è reperibile in formato digitale all'indirizzo https://webcontat.umbriasalute.com/webcontat/ nella sezione "Ris. Umane"
- "Umbria Salute e Servizi S.c.a r.l.", Umbria Digitale S.c.a r.l.","Webred S.p.a.", : vecchie ragioni sociali di PUNTOZERO, ancora reperibili nella documentazione del Sistema Qualità.
- "Struttura": Insieme organizzativo
- "DCRU": Data Center Regionale Unitario
- C.U.P. = Centro Unificato Prenotazioni
- "SoA": Statement of Applicability contiene l'insieme dei controlli relativi al trattamento dei rischi connessi alla sicurezza delle informazioni
- "AgID": Agenzia per l'Italia Digitale
- "PSN": Polo strategico Nazionale
- "CSP": cloud service provider

1. INTRODUZIONE

Il presente documento definisce, al livello più alto di sintesi, gli elementi che costituiscono nel loro insieme il Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni (SGQ) adottato in azienda.

Fornisce tutti gli elementi del SGQ che riguardano aspetti organizzativi, i processi interessati e le procedure adottate.

La presente versione differisce dalla precedente in quanto a seguito della fusione per incorporazione di Umbria Digitale scarl in Umbria Salute e Servizi scarl e del contestuale cambio di ragione sociale di Umbria Salute e Servizi scarl in PuntoZero scarl, a partire dal 1° gennaio 2022 si amplia il campo di applicazione della certificazione includendo i processi di Progettazione, sviluppo e installazione di sistemi informativi, erogazione di servizi di conduzione tecnica, operativa e funzionale di sistemi informativi gestiti nel Data Center Regionale Unitario (DCRU) e l'erogazione di servizi Cloud in modalità IAAS e il processo di erogazione di servizi di acquisto in qualità di centrale regionale acquisti per la Sanità (CRAS)

L'aggiornamento della ragione sociale viene effettuato, al momento, solo nel presente documento, in quanto rappresenta il documento di più alto livello del sistema qualità aziendale, mentre si provvederà alla progressiva sostituzione negli altri documenti del SGQ, in occasione del loro naturale processo di revisione.

2. PRESENTAZIONE DELL'AZIENDA

PuntoZero scarl è la società consortile a totale capitale pubblico sottoscritto integralmente dalla Regione, dalle Aziende sanitarie regionali e dalle altre pubbliche amministrazioni operanti sul territorio, costituita dal 1° gennaio 2022 a seguito del cambio di ragione sociale di Umbria Salute e Servizi scarl e la fusione per incorporazione di Umbria Digitale scarl.

Pertanto da tale data Umbria Salute e Servizi Scarl (che contestualmente ha assunto la denominazione di "Punto Zero S.c.a r.l.") subentra senza soluzione di continuità ed a pieno titolo, ai sensi degli artt. 2504 e seguenti c.c., in tutto il patrimonio attivo e passivo, nonché in tutti i rapporti giuridici attivi e passivi, ivi compresi i rapporti di lavoro, azioni, diritti, licenze, autorizzazioni così come in tutti gli obblighi ed impegni di qualsiasi natura della Società incorporata. A seguito della suindicata operazione di fusione per incorporazione, dalla data del 01.01.2022 risulta operativa la sola "PuntoZero S.c.ar.l."

La Società non ha scopo di lucro, ma quello di istituire una organizzazione e strutture comuni a servizio della Regione Umbria, delle Aziende Sanitarie Regionali, dei Comuni, delle Agenzie o organismi pubblici in essa consorziati al fine di conseguire maggiori snellezze ed efficienze operative e risparmi gestionali.

3. CONTESTO DELL'ORGANIZZAZIONE

3.1 Comprendere l'organizzazione e il suo contesto

PUNTOZERO determina, verifica e riesamina costantemente le problematiche interne ed esterne che possono avere effetti sulla capacità del Sistema di Gestione Integrato (SGQ) di raggiungere i risultati previsti.

3.1.1 Analisi del contesto esterno

La società eroga servizi di interesse generale, quali:

- sviluppo dell'innovazione tecnologica e gestione della transizione al digitale del sistema pubblico regionale e dei relativi flussi informativi;
- cura le attività per l'erogazione dei servizi preordinati alla tutela della salute;
- agisce per la produzione di beni e la fornitura di servizi rivolti all'utenza e cura la gestione dei flussi informativi del sistema sanitario regionale;
- ha la responsabilità dello sviluppo e gestione del data center regionale e della rete pubblica e conduzione di sistemi e flussi informativi a valenza regionale e nazionale
- cura e gestisce l'Osservatorio epidemiologico regionale

L'attività di interesse generale si svolge anche mediatamente, tramite l'erogazione di servizi strumentali alle attività istituzionali delle Amministrazioni socie quali il supporto tecnico-operativo a favore delle strutture amministrative degli enti soci e l'erogazione di servizi ICT nell'ambito delle organizzazioni interne dei singoli enti soci. La Società svolge anche funzioni di Centrale d'acquisto per l'approvvigionamento di beni, servizi e lavori a favore delle pubbliche amministrazioni e degli enti soci e di soggetto aggregatore ai sensi del D.L. n. 66/2014 convertito in Legge n. 89/2014 e ss.mm.

La Società non ha scopo di lucro, ma quello di istituire una organizzazione e strutture comuni a servizio della Regione Umbria, delle Aziende Sanitarie Regionali, dei Comuni, delle Agenzie o organismi pubblici in essa consorziati al fine di conseguire maggiori snellezze ed efficienze operative e risparmi gestionali.

La società ha l'obiettivo generale di erogare ai propri soci servizi informatici/informativi quali:

- Progettazione e realizzazione dei servizi (Service Design)
- Gest. operativa Servizi IT (infrastrutturali e applicativi)

- Gestione della Sicurezza informatica (Information Security Management)
- Servizi di Front Office (attività di sportello CUP)
- Servizi di Back Office (supporto)
- Assistenza agli utenti (di I° e II° livello)
- Approvvigionamento di servizi, lavori e forniture in qualità di Centrale d'acquisto (CRA/CRAS)

Nel raggiungimento di tale obiettivo, PUNTOZERO assicura ai propri stakeholder livelli qualitativi e di sicurezza nel trattamento e nella protezione dei dati gestiti, anche in funzione dell'ottemperanza alla normativa UE 2106/679 sulla protezione dei dati personali (cd GDPR). Tali livelli qualitativi e di sicurezza sono stati inoltre attestati da AgID, in data 10 febbraio 2020, mediante la classificazione del DCRU come candidabile a Polo Strategico Nazionale - PSN.

PuntoZero inoltre, a fronte dei requisiti richiesti dalla regione dell'Umbria nel contratto di servizio (PdE) e in specifici progetti, si è dotata di un Sistema di gestione integrato per la Qualità e la Sicurezza delle informazioni (SGQ), conforme alle norme ISO 9001:2015 e, per quanto riguarda il Data Center Regionale Unitario (DCRU), alle norme ISO/IEC 27001:2013, 27017:2015 e 27018:2019.

3.1.2 Analisi del contesto interno

La Società, al fine di conseguire l'obiettivo generale sopra descritto, è strutturata in Processi e strutture organizzative alle quali fanno capo attività specifiche con propri responsabili.

Il contesto interno è caratterizzato dalla:

- *la fusione* che necessita di un cambio di prospettiva da parte del personale al fine di iniziare a mettere in atto le azioni necessarie per conseguire la visione aziendale. Questo cambio deve essere supportato da una adeguato processo di change management per fare in modo che l'esercizio del ruolo, a tutti i livelli, sia coerente con al nuova mission e vision aziendale;
- *le nuove strategie* che caratterizzano ogni area aziendale che hanno lo scopo di definire il come poter procedere per l'erogazione dei servizi coerentemente con la vision aziendale;
- *Valorizzazione delle risorse umane: v*iene riconosciuta la centralità delle risorse umane nella convinzione che il principale fattore di successo dell'impresa sia costituito dal contributo professionale delle persone che vi operano.

3.2 Comprendere le esigenze e le aspettative delle parti interessate

3.2.1 Le parti interessate rilevanti per il SGQ Qualità e Sicurezza delle Informazioni

Al fine di comprendere le esigenze e le aspettative delle parti interessate il primo passo consiste nel determinare le categorie di portatori di interesse. Quelle individuate ai fini della gestione aziendale sono le seguenti:

Soci - Parità di trattamento a tutti i soci evitando comportamenti preferenziali. I reciproci vantaggi derivanti dall'appartenenza al consorzio vengono perseguiti nel rispetto delle normative applicabili e dell'interesse autonomo di ciascun socio alla creazione di valore.

Disporre di un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni rappresenta un valore determinante per l'immagine del servizio pubblico.

Responsabili dei servizi degli Enti Soci - Sono i soggetti che rispondono direttamente alla loro direzione e ai cittadini circa la qualità dei servizi prestati dagli operatori di PUNTOZERO.

Un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni è un elemento rassicurante per chi deve erogare servizi alla collettività.

Utenti del sistema informativo all'interno degli enti soci (utenti interni) – L'obiettivo perseguito è quello di garantire una risposta immediata, qualificata e competente alle esigenze degli utenti, improntando i propri comportamenti a correttezza, cortesia e collaborazione.

Un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni contribuisce alla certezza del risultato fornito dai vari applicativi utilizzati.

Comunità (utenti esterni ovvero imprese, professionisti, cittadini, etc.) - La società tiene in considerazione ed è consapevole della rilevanza sociale del servizio erogato all'utenza e delle conseguenti responsabilità verso la collettività e la comunità in genere.

Inoltre la società garantisce pari opportunità, nel rispetto dei principi della trasparenza e della prevenzione della corruzione (o *maladministration*), ai soggetti partecipanti ai bandi per l'acquisizione di beni, lavori, servizi e competenze.

Un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni trasparente agli utilizzatori finali, garantisce risultati e prestazioni in linea con le attese.

Dipendenti e sindacati - La gestione dei rapporti di lavoro è orientata a garantire pari opportunità ed a favorire la crescita professionale di ciascuno nonché la soddisfazione dei dipendenti rispetto all'organizzazione e al clima interno.

Un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni permette garantisce le giuste competenze in funzione dei servizi richiesti

Istituti di credito – La gestione amministrativa dell'azienda prevede il ricorso a finanziamenti bancari. E' interesse anche di detti operatori che l'azienda sia affidabile ed i risultati economici siano solidi e permettano alla stessa di operare nel rispetto degli obiettivi di bilancio prefissati.

Un sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni è un elemento rassicurante in termini di affidabilità dell'azienda e quindi della sua solidità.

Fornitori - Il loro interesse è che l'azienda abbia attività consolidate, che continui a fare ordini presso di loro e che i pagamenti siano puntuali. Altro interesse primario è che gli ordini che gli vengono inoltrati siano chiari e comprendano tutte le informazioni necessarie per lavorare.

Un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni fornisce garanzie sul controllo degli accessi logici alle risorse permettendo di definire specifiche responsabilità.

A questo gruppo è opportuno aggiungere anche i soggetti che vigilano sulle attività della società, affinché il suo operato si realizzi nel rispetto delle leggi vigenti, cercando di evitare possibilità di incorrere in illeciti passibili di sanzioni sul piano penale e amministrativo, oltre ai soggetti interessati dalle attività di CRAS:

Organi di controllo (DPO - RPCT - Revisore dei conti) - L'organizzazione del controllo interno ha lo scopo di garantire, preventivamente, che gli organi di Amministrazione attiva operino per il perseguimento dei fini ad essi assegnati attraverso l'uso di poteri, procedure e risorse sempre legislativamente deliberate. Sono di interesse di questi organi: la regolarità amministrativa e contabile e la legittimità della stessa.

CRAS:

- **Assessorato/Direzione Salute Regione Umbria** - Aspettative: Coordinamento attività di programmazione gare centralizzate ed espletamento gare programmate di acquisizione di beni e servizi sanitari e non
- **Aziende sanitarie ed ospedaliere Regione Umbria** (Direzioni, provveditorati, dipartimenti farmaceutici, professionisti sanitari) - Aspettative: Espletamento gare programmate di acquisizione di beni e servizi sanitari e non
- **Aziende fornitrici di beni e servizi sanitari e non** - Aspettative: corretto, efficiente ed efficace espletamento delle gare espletate
- **Ministero Economia e Finanze/ANAC** - Aspettative: copertura totale delle merceologie riservate ai Soggetti Aggregatori, corretto, efficiente ed efficace espletamento delle gare espletate
- **Tavolo Soggetti Aggregatori** (articolo 9 del decreto legge 24 aprile 2014, n. 66) - Aspettative: partecipazione alle attività istituzionali, di studio, di elaborazione documenti per esigenze congiunte e di proposta ad altri soggetti istituzionali

4. IL CAMPO DI APPLICAZIONE DEL SGQ QUALITÀ E SICUREZZA DELLE INFORMAZIONI

Coerentemente con l'analisi del contesto effettuata, della definizione dei portatori di interesse e della salvaguardia dei requisiti delle parti interessate è stato definito il seguente campo di applicazione del sistema di Gestione della Qualità:

"Progettazione sviluppo e installazione di sistemi informativi. Progettazione ed erogazione di servizi di conduzione tecnica, operativa e funzionale di sistemi informativi, servizi di front-office (presidio telefonico e di sportello) e di back-office, in sede o localizzati secondo le necessità del cliente. Erogazione di Servizi in qualità di centrale regionale per gli acquisti in sanità anche come soggetto aggregatore.

In ambito di Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni, sovrapposto al precedente campo di applicazione, che descrive gli ambiti tecnologici, è stato definito il presente perimetro di applicazione:

"Erogazione di servizi di conduzione tecnica, operativa e funzionale di sistemi informativi gestiti nel Data Center Regionale Unitario (DCRU)". Erogazione di servizi Cloud in modalità IAAS con l'utilizzo delle Linee Guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

Nel documento "SoA - Statement of applicability", ampliato con i controlli previsti dalle linee guida ISO 27017 e ISO 27018, sono descritti i criteri di esclusione delle parti non ricomprese nel perimetro.

Pertanto il presente documento è indirizzato a tutto il personale che dirige, esegue e verifica attività che influenzano la qualità in tali aree di applicazione.

Per l'ambito di applicazione del sistema di gestione della Qualità non sono previste esclusioni, mentre, per il sistema di gestione della Sicurezza delle informazioni, la sua applicazione è prevista al momento al solo Data Center Regionale Unitario (DCRU), escludendo la progettazione delle applicazioni software.

5. I PROCESSI AZIENDALI

Al fine di rispondere alle esigenze di servizio richieste dagli enti soci, PUNTOZERO ha definito una serie di processi interni aventi caratteristiche e meccanismi diversi uno dall'altro, ma tutti orientati al raggiungimento degli obiettivi dell'organizzazione.

L'applicazione dell'approccio per processi all'interno del SGQ permette:

a) di comprendere i requisiti e di soddisfarli in modo coerente;

b) di considerare i processi in termini di valore aggiunto;

c) il conseguimento di efficaci prestazioni di processo;

d) l'implementazione di un metodo efficace di gestione basato sul *risk-based thinking*;

e) il miglioramento dei processi sulla base della valutazione di dati e informazioni.

Si riporta di seguito la mappatura dei processi PuntoZero:

Mappatura Processi

<table>
<tr><td>Strategici</td><td colspan="5">Processo strategico direzionale</td></tr>
<tr><td>Core</td><td colspan="5">Realizzazione ed erogazione dei servizi ICT
Acquisti (CRAS e Acquisti interni)
Servizi all'utenza
Servizi di Supporto Specialistico[1]
Sviluppo strategie e politiche di riuso ed extra soci[2]</td></tr>
<tr><td>Supporto</td><td>Gestione Risorse umane</td><td>Contabilità e bilancio</td><td>Affari legali e contenzioso</td><td>Qualità</td><td>Comunicazione</td></tr>
</table>

[1] Processo non ricompreso nel perimetro di certificazione
[2] Processo non ricompreso nel perimetro di certificazione

Di seguito per ogni processo vengono riportati i relativi sottoprocessi:

N.	Processo	Sub-Processo
1	Processo strategico direzionale	Processo strategico direzionale
2	Gestione Risorse umane	Gestione competenze e formazione
		Selezione e assunzione del personale e conferimento incarichi esterni
3	Contabilità e bilancio	Amministrazione finanziaria
		Contabilità e bilancio
4	Affari legali e contenzioso	Affari legali e contenzioso
5	Acquisti (CRAS e Acquisti interni)	Acquisti (CRAS e Acquisti interni)
6	Qualità	Gestione Sistema Qualità e miglioramento
		Gestione del rischio
7	Comunicazione	Comunicazione
8	Servizi all'utenza	Servizi di Front Office
		Servizi di Back Office (supporto)
		Assistenza agli utenti (L1 e L2)
9	Realizzazione ed erogazione dei servizi ICT	Progettazione e realizzazione dei servizi (SERVICE DESIGN)
		Gest. operativa Servizi IT (infrastrutturali e applicativi)
		Gestione della Sicurezza informatica (INFORMATION SECURITY MANAGEMENT)
10	*Sviluppo strategie e politiche di riuso ed extra soci*	*Sviluppo strategie e politiche di riuso ed extra soci*
11	*Servizi di supporto specialistico*	*Servizi di supporto specialistico*

Le schede di ciascun processo, secondo lo schema sopra riportato, sono contenute nell'area della Intranet aziendale (Google Workspace) sotto la voce di menù "Sistema Documentale Aziendale - Processi aziendali" e disponibile per la consultazione a tutto il personale.

6. RUOLI E RESPONSABILITÀ NELL'ORGANIZZAZIONE

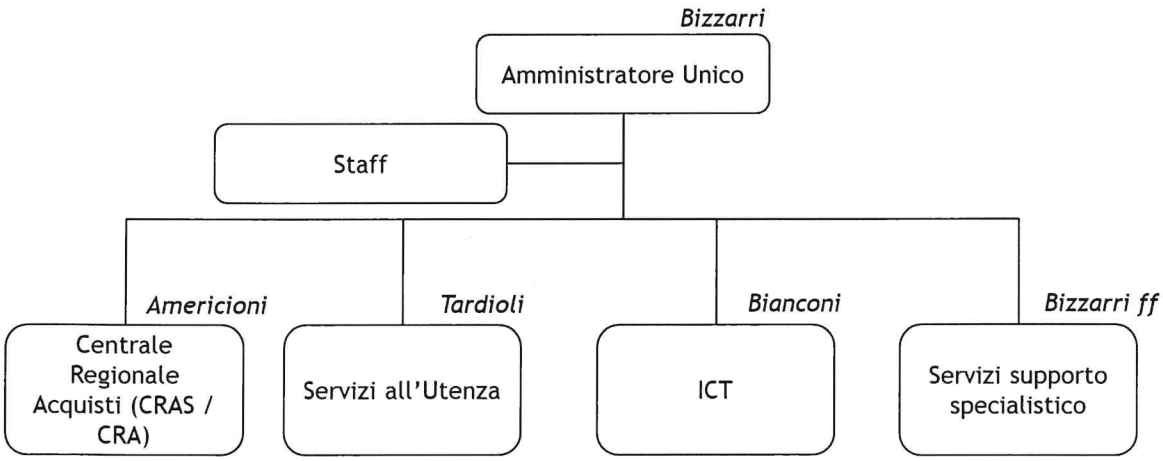
La Direzione definisce e comunica le responsabilità e le autorità per l'attuazione di sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni che sia efficace ed efficiente e per il suo mantenimento, assicurando altresì l'integrazione dei requisiti di Qualità e Sicurezza delle Informazioni nei processi aziendali.

L'organizzazione ed i ruoli previsti per l'applicazione delle procedure del SGQ sono descritti in appositi ordini di servizio, diffusi in varie forme a tutto il personale e disponibili nel sistema documentale aziendale nella loro ultima versione.

Da tale documento sono desumibili le strutture organizzative coinvolte nell'esercizio del SGQ e le responsabilità assegnate all'interno dei processi aziendali.

La responsabilità delle attività che influenzano la qualità dei prodotti/servizi forniti da PUNTOZERO S.c.a r.l. e dell'applicazione delle politiche del SGQ, è dell'Amministratore Unico.

Di seguito la rappresentazione schematica del nuovo modello organizzativo:



con il dettaglio delle aree di staff:

Coerentemente con la vision aziendale, le strategie che le aree produttive dovranno sviluppare per creare valore, sono le seguenti:

Area ICT - Essere il motore dell'innovazione digitale della Regione

CRAS - Essere ed avere un ruolo di coordinamento e governo delle procedure di approvvigionamento a livello Regionale

CRA - Avviare gli acquisti nella PA al fine di ottenere economie di scala

Servizi all'utenza - Diventare il gestore delle modalità di accesso del cittadino per la specialistica ambulatoriale per fornire gli strumenti ed i dati per il governo delle Liste di Attesa da parte delle Aziende

Come da Modello Organizzativo, le quattro unità operative dovranno occuparsi delle seguenti attività:

- **ICT**, nella quale sono previste le attività definite all'art. 2 comma 3 punto a) c) d) LR 2 agosto 2021 n.13, ovvero le attività rese per lo sviluppo dell'innovazione tecnologica e gestione della transizione al digitale del sistema pubblico regionale e dei relativi flussi informativi, anche mediante la digitalizzazione del Sistema Informativo Sanitario Regionale e del Sistema Informativo Regionale, lo sviluppo e la gestione del Data Center Regionale e della Rete Pubblica Regionale, la progettazione, direzione, integrazione e conduzione di sistemi e flussi informativi a valenza regionale e nazionale.

- **Centrale Regionale di Acquisto,** nella quale sono incluse le attività di soggetto aggregatore quelle relative alla centrale di acquisto per il Sistema Sanitario Regionale (CRAS) e quelle afferenti la centrale di acquisto per il sistema pubblico regionale (CRA) come definito dagli ambiti dell'art.4 comma 3 LR 2 agosto 2021 n.13.s
- **Servizi all'Utenza,** nella quale è prevista la produzione di beni e la fornitura di servizi rivolti all'utenza compresa l'attività di front office di servizi al cittadino, l'attività di Back Office dei servizi rivolti all'utenza del Sistema Sanitario Regionale nonché le attività dei servizi di Contact Center, in cui sono inclusi le attività afferenti il Numero Unico Enti e quelle di Help Desk.
- **Servizi di Supporto Specialistico,** nella quale sono incluse le attività definite all'art.2 comma 3 punto e) della Legge 2 agosto 2021 n.13 dell'Osservatorio Epidemiologico attraverso la cura dei relativi flussi informativi.

L'attività di interesse generale svolta tramite l'erogazione di servizi strumentali alle attività istituzionali delle amministrazioni socie, quali supporto tecnico operativo a favore delle strutture amministrative degli enti soci e l'erogazione dei servizi inerenti le tecnologie dell'informazione e della comunicazione, sono riattribuite in funzione dell'utilizzo ai rispettivi ambiti operativi sopra elencati.

Oltre all'organizzazione è importante definire i processi/sub-processi di PuntoZero scarl ed i relativi owner:

N.	Processo	Owner	Sub-Processo	Owner
1	Processo strategico direzionale	Amministratore Unico	Processo strategico direzionale	Amministratore Unico
2	Gestione Risorse umane	Dirigente resp. Risorse Umane, Amm.ne e Controllo	Gestione competenze e formazione	Dirigente resp. Risorse Umane
			Selezione e assunzione del personale e conferimento incarichi esterni	Dirigente resp. Risorse Umane
3	Contabilità e bilancio	Dirigente resp. Risorse Umane, Amm.ne e Controllo	Amministrazione finanziaria	Dirigente resp. Amm.ne e Controllo
			Contabilità e bilancio	Dirigente resp. Amm.ne e Controllo
4	Affari legali e contenzioso	Dirigente Servizi Legali, Societari e Privacy	Affari legali e contenzioso	Dirigente Servizi Legali, Societari e Privacy
5	Acquisti (CRAS e Acquisti interni)	Dirigente CRAS	Acquisti (CRAS e Acquisti interni)	Dirigente CRAS
6	Qualità	Responsabile Qualità	Gestione Sistema Qualità e miglioramento	Responsabile Qualità

			Gestione del rischio	Responsabile Qualità
7	Comunicazione	Area Comunicazione	Comunicazione	Area Comunicazione
8	Servizi all'utenza	Resp. Servizi all'Utenza	Servizi di Front Office	Responsabile CUP e servizi di supporto
			Servizi di Back Office (supporto)	Responsabile CUP e servizi di supporto
			Assistenza agli utenti (L1 e L2)	Resp. Contact Center
9	Realizzazione ed erogazione dei servizi ICT	Resp. ICT	Progettazione e realizzazione dei servizi (SERVICE DESIGN)	Resp. ICT
			Gest. operativa Servizi IT (infrastrutturali e applicativi)	Resp. ICT
			Gestione della Sicurezza informatica (INFORMATION SECURITY MANAGEMENT)	Resp. Cyber Security
10	*Sviluppo strategie e politiche di riuso ed extra soci*	*Dirigente resp. Amministrazioni Esterne e Riuso*	*Sviluppo strategie e politiche di riuso ed extra soci*	*Dirigente resp. Amministrazioni Esterne e Riuso*
11	*Servizi di supporto specialistico*	*Amministratore Unico (ad interim)*	*Servizi di supporto specialistico*	*Amministratore Unico (ad interim)*

Ai fini di un'efficace azione per la garanzia della qualità e della sicurezza delle informazioni, sono definiti inoltre i seguenti ruoli:

- Responsabile Sistema Qualità
- Responsabile struttura aziendale/Responsabile processo
- Ispettore Qualità e Sicurezza delle Informazioni

Responsabile Sistema Qualità

Coordina le attività di pianificazione, armonizzazione, integrazione e supporto alla realizzazione e gestione del Sistema Qualità e Sicurezza delle informazioni. Risponde direttamente alla direzione.

Le responsabilità attribuite alla funzione sono:

Sistema

- sviluppare e mantenere il Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni (SGQ) assicurando costantemente la coerenza con le norme di riferimento;
- curare la distribuzione controllata della documentazione relativa al SGQ;

- pianificare e assicurare l'avanzamento delle verifiche ispettive sull'applicazione del SGQ con particolare attenzione ad eventuali situazioni di criticità;
- assicurare che il SGQ, visto nel suo complesso, operi efficacemente;
- valutare ed accogliere i suggerimenti per intraprendere iniziative, atte al miglioramento e alla revisione del sistema, al fine di impostare nuovi programmi per la qualità;
- curare l'impostazione di un sistema di metriche sulla qualità dei vari processi del SGQ;
- scegliere gli Ispettori della Qualità e della Sicurezza delle Informazioni;
- partecipare alle riunioni di riesame, predisponendo la documentazione per quanto riguarda il SGQ e il relativo verbale;
- mantenere i contatti con l'organismo di certificazione: in particolare, comunicare le modifiche e gli aggiornamenti del SGQ e della relativa documentazione, fornire adeguato supporto alla pianificazione delle attività di ispezione e garantire agli Ispettori dell'organismo di certificazione l'accesso alle opportune strutture;
- sviluppare, in collaborazione con i responsabili di processo, adeguati interventi formativi sulle problematiche connesse al SGQ.

Processi aziendali

- garantire che la pianificazione della qualità venga effettuata per ogni processo e che i requisiti per la Qualità e la Sicurezza delle informazioni siano singolarmente identificabili;
- analizzare, sulla base dei dati relativi alla qualità dei prodotti/servizi forniti dalle strutture operative, il livello qualitativo delle forniture e monitorare quindi l'efficienza e l'efficacia del processo;

Responsabile struttura aziendale/Responsabile processo

Nell'Organizzazione è assicurato il controllo della qualità e della sicurezza delle informazioni sui prodotti/servizi mediante verifica della qualità dei processi.

E' compito dei responsabili delle strutture che gestiscono i processi loro assegnati assicurare che il controllo qualità sia effettuato secondo quanto previsto dalle procedure del SGQ e dagli specifici piani della qualità.

In particolare questi hanno la responsabilità di:

- garantire che i prodotti/servizi forniti ai soci e agli utenti finali rispettino le quanto previsto indicazioni espresse nei piani della qualità;
- fornire supporto al personale nell'utilizzo del SGQ in qualsiasi fase del processo produttivo gestito;

- definire la documentazione necessaria per lo svolgimento dei processi condotti (procedure, istruzioni operative, moduli, etc.) e curarne il costante aggiornamento;
- svolgere le attività di controllo qualità e individuare le risorse da assegnare a tali attività garantendo che queste abbiano esperienze e conoscenze adeguate;
- mantenere registrazione dei controlli effettuati, del loro esito e delle azioni correttive adottate;
- stabilire, d'intesa con il responsabile SGQ, le azioni necessarie e le modifiche al sistema gestione qualità;
- fornire al responsabile SGQ i dati relativi alla qualità dei prodotti/servizi e segnalare eventuali problemi riscontrati nell'utilizzo dell'applicazione del SGQ.

Il controllo della qualità e della sicurezza delle informazioni avviene durante l'intero processo produttivo e si esplica attraverso:

- verifiche sui documenti che formalizzano i risultati delle attività;
- riesami formalizzati dei risultati della progettazione;
- validazione del servizio, ove praticabile, prima della consegna al cliente/committente;
- controllo dei livelli di servizio erogato;
- rispetto delle procedure previste per la gestione della sicurezza delle informazioni in particolare in relazione alle informazioni di identificazione personale aggiornate in funzione dell'erogazione dei servizi in modalità cloud

Ispettore Qualità e Sicurezza delle Informazioni

Riporta funzionalmente al Responsabile SGQ ed ha il compito di eseguire le verifiche ispettive; pertanto ha la responsabilità di:

- preparare le verifiche ispettive;
- effettuare le verifiche ispettive, redigere i rapporti relativi e verificare il completamento e l'esito di eventuali azioni correttive concordate in sede di ispezione;
- fornire supporto, all'interno della propria struttura, per l'applicazione degli standard e delle procedure del SGQ;
- riferire al Responsabile SGQ sui problemi riscontrati nell'applicazione degli standard e delle procedure del SGQ.

7. POLITICA INTEGRATA PER LA QUALITÀ E LA SICUREZZA DELLE INFORMAZIONI

Punto Zero S.c. a r.l. è la società consortile a totale capitale pubblico sottoscritto integralmente dalla Regione, dalle Aziende sanitarie regionali e dalle altre pubbliche amministrazioni operanti sul territorio.

La società, eroga servizi di interesse generale, quali:

- *sviluppo dell'innovazione tecnologica e gestione della transizione al digitale del sistema pubblico regionale e dei relativi flussi informativi;*
- *cura le attività per l'erogazione dei servizi preordinati alla tutela della salute;*
- *agisce per la produzione di beni e la fornitura di servizi rivolti all'utenza e cura la gestione dei flussi informativi del sistema sanitario regionale;*
- *ha la responsabilità dello sviluppo e gestione del data center regionale e della rete pubblica e conduzione di sistemi e flussi informativi a valenza regionale e nazionale*
- *cura e gestisce l'Osservatorio epidemiologico regionale*

L'attività di interesse generale si svolge anche mediatamente, tramite l'erogazione di servizi strumentali alle attività istituzionali delle Amministrazioni socie quali il supporto tecnico-operativo a favore delle strutture amministrative degli enti soci e l'erogazione di servizi ICT nell'ambito delle organizzazioni interne dei singoli enti soci. La Società svolge anche funzioni di Centrale d'acquisto per l'approvvigionamento di beni, servizi e lavori a favore delle pubbliche amministrazioni e degli enti soci e di soggetto aggregatore ai sensi del D.L. n. 66/2014 convertito in Legge n. 89/2014 e ss.mm. e II. di cui meglio al successivo Art. 6

La società eroga ai propri soci/clienti servizi informativi/informatici, servizi di front-office (presidio telefonico e di sportello) e di back-office nonché cura l'approvvigionamento di servizi, lavori e forniture in qualità di Centrale d'acquisto.

Nell'erogazione di tali servizi, Punto Zero S.c. a r.l., al fine del perseguimento degli obiettivi di Qualità e della Sicurezza delle Informazioni, sviluppa e gestisce un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle informazioni (SGQ) che governa l'insieme dei requisiti previsti dalle norme ISO 9001, ISO 27001, ISO 27017 e ISO 27018.

L'organizzazione identifica le proprie attività come processi da pianificare, controllare e migliorare costantemente e attiva al meglio le risorse per la loro realizzazione. L'organizzazione gestisce i propri processi perché siano univoci:

- *gli obiettivi da perseguire e i risultati attesi;*
- *le responsabilità connesse e le risorse impiegate.*

I servizi erogati da Punto Zero S.c. a r.l. sono pertanto strutturati secondo il seguente schema dei processi:

- *Realizzazione ed erogazione dei servizi ICT*
- *Servizi all'utenza*
- *Sviluppo strategie e politiche di riuso ed extra soci*
- *Acquisti (CRAS e Acquisti interni)*

Mission

La società si propone come strumento di sistema per la realizzazione delle strategie Regionali volte al miglioramento della governance e dei processi di erogazione dei servizi ai cittadini,

Vision

Diventare un supporto Regionale per l'innovazione del Sistema Sanitario Regionale e della Pubblica Amministrazione.

I nostri valori

Sono quelli che devono guidare i comportamenti del personale di Punto Zero S.c. a r.l allineandoli alla vision aziendale:

Ne consegue che, nella gestione delle proprie attività, Punto Zero S.c. a r.l:

- *garantisce la **presa in carico** dei problemi sino alla loro soluzione puntuale ed estensione ai processi aziendali interessati a livello di sistema azienda*
- *si attiene ai più rigorosi **principi di etica** professionale nello svolgimento dei servizi ad essa affidati ed in ogni altro settore delle proprie attività;*
- *assicura il principio di **massima trasparenza** nel rapporto con gli enti soci ed in generale con gli stakeholder*
- *favorisce il **coinvolgimento di tutte le componenti aziendali** nelle decisioni*
- *stimola il **confronto** tra il personale garantendo le pari opportunità e la **crescita professionale** di ciascuno*
- *Progetta il **cambiamento** al fine di migliorare l'erogazione dei servizi*
- ***Introduce innovazione,** in funzione delle esigenze dell'utenza, sia essa imprese o cittadini.*

Il nostro impegno per la qualità

L'obiettivo principale di Punto Zero S.c. a r.l è quello di raggiungere la piena soddisfazione dei clienti/soci e degli utenti finali dando prova di essere:

- ***Proattiva**: intercettando i problemi prima che generino perdita di efficienza ed efficacia nei servizi erogati*
- ***Competente**: sviluppando idee innovative per il sistema umbro.*
- ***Affidabile**: rispettando gli impegni e facendo ciò che dichiara affinché i nostri utenti possano fidarsi di noi;*

L'obiettivo di rispondere alle esigenze delle pertinenti parti interessate è perseguito inoltre:

- *ragionando in una logica di sistema regionale al fine di ottimizzare le risorse e massimizzare la diffusione dei servizi innovativi*
- *prestando attenzione, nello svolgimento dei processi interni, al fine di preservarne i requisiti e prevenirne i difetti;*
- *agendo in base al principio che i processi devono essere governati attraverso il monitoraggio delle performance e dei rischi*
- *mantenendo una elevata sensibilità ai bisogni, alle aspettative e alle informazioni di ritorno dalle stesse, cercando di anticiparli con un approccio proattivo;*
- *credendo nel miglioramento continuo (sia interno, che dei servizi ai cittadini, che degli strumenti di governo) come elemento di coinvolgimento del personale;*
- *mantenendo un unico sistema aziendale che sia integrato per i diversi ambiti di gestione della Qualità e la Sicurezza delle informazioni;*

La competenza e la professionalità del personale, la loro motivazione e coinvolgimento continuo nei processi aziendali, la consapevolezza della rilevanza e dell'importanza delle proprie attività sono condizioni fondamentali per il conseguimento degli obiettivi societari.

Il nostro impegno per la sicurezza delle informazioni

Punto Zero S.c. a r.l. si impegna ad adottare gli standard ed i livelli di sicurezza più idonei per i dati trattati, garantendo al contempo performance ottimali dei servizi erogati. Analoga attenzione alla sicurezza (principi del privacy by design e privacy by default) è prestata nella progettazione e realizzazione dei servizi innovativi.

La Società, nel trattamento delle informazioni, si ispira infatti ai principi di:

- ***riservatezza**: le informazioni devono essere conosciute solo da coloro che ne hanno il relativo diritto, rispettando il principio del minimo privilegio ("necessità di sapere") in base alle mansioni ricoperte ("necessità di operare");*
- ***integrità**: le informazioni devono essere precise e complete, devono rispettare i valori e le aspettative aziendali, e devono essere protette da modifiche e cancellazioni non autorizzate. Per soddisfare tale requisito le informazioni devono essere esatte, aggiornate e leggibili;*
- ***disponibilità**: le informazioni devono essere disponibili quando richiesto dai processi aziendali, in maniera efficace ed efficiente;*
- ***efficacia**: le informazioni devono essere rilevanti e pertinenti al processo aziendale e, allo stesso tempo, devono essere disponibili tempestivamente, senza errori e fornite in modo da poter essere utilizzate dall'utente;*
- ***efficienza**: le informazioni devono essere fornite attraverso l'uso ottimale delle risorse sia dal punto di vista della produttività che della economicità;*

Punto Zero S.c. a r.l si impegna altresì a trattare i dati personali:

- *in osservanza dei criteri di riservatezza;*
- *in modo lecito e secondo correttezza;*
- *per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;*
- *nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

La Società predispone ed implementa il proprio Piano di Continuità Operativa ed il Piano di Disaster Recovery. Obiettivo dell'azienda è assicurare la protezione dei dati e dei sistemi contro le possibili conseguenze dell'attività di software dannoso (c.d. malware). Inoltre, la Società, tenuto conto della particolare criticità dei ruoli connessi alla gestione del Sistema Informativo, adotta idonee cautele volte a prevenire e ad accertare eventuali utilizzi non in linea con gli obiettivi aziendali.

Enfasi particolare è posta ai servizi contrattualizzati in tecnologia cloud. A tal fine, ai rispetto dei requisiti del sistema di gestione della sicurezza delle informazioni ISO 27001, sono aggiunti i requisiti previsti dalle norme ISO 27017 e ISO 27018.

8. OBIETTIVI E INDICATORI PER LA QUALITÀ E PIANIFICAZIONE PER IL LORO RAGGIUNGIMENTO

Gli obiettivi discendono dalle strategie mentre la Politica per la qualità e la sicurezza delle informazioni rappresentano il come ci si deve comportare per il conseguimento degli obiettivi Gli obiettivi si realizzano attraverso i processi, le risorse e le strutture organizzative previste per il loro raggiungimento.

Tali obiettivi rappresentano un quadro di riferimento per l'organizzazione, si traducono in obiettivi operativi, misurabili e finalizzati al miglioramento delle prestazioni dell'organizzazione e inseriti nei piani di lavoro.

Le aree di lavoro sono organizzate per processi, pertanto sono stati definiti indicatori omogenei che consentano di misurare la capacità delle aree di generare valore ovvero di raggiungere gli obiettivi.

Le misure individuate, sono funzionali a:

- valutare lo stato di raggiungimento di un obiettivo
- tenere sotto controllo il processo/prestazione
- identificare le opportunità di miglioramento

Il raggiungimento degli obiettivi prefissati viene valutato mediante l'esame delle metriche riportate nel documento "*Obiettivi Personale Punto Zero*" (disponibile al link

https://docs.google.com/spreadsheets/d/1MWa5jJ4tkmYXV8n8Q86CzhKTSswELSpjSGKYPpUuhgY/edit?usp=sharing) che costituisce il catalogo degli obiettivi aziendali ed i relativi indicatori, definiti specificatamente per il personale di ogni struttura aziendale. Tali obiettivi sono connessi agli obiettivi dei responsabili delle strutture operative che hanno anche ulteriori obiettivi specifici.

Il sistema degli obiettivi aziendali infatti, fa sì che a cascata gli obiettivi dell'Amministratore Unico vengano declinati sugli obiettivi dei responsabili aziendali e questi connessi a quelli del personale.

Il sistema degli obiettivi è anche connesso alla premialità aziendale (mediante accordo formalizzato con le organizzazioni sindacali)

Concorre altresì, al raggiungimento degli obiettivi generali, il rispetto di specifici livelli di servizio (SLA) eventualmente contrattualizzati con i soci (si veda il documento 'zq-00-q0-04 - Mappa dei documenti SLA (Dizionario SLA)'.

Le metriche ed i report SLA sono di norma analizzate dai responsabili delle strutture responsabili dei processi (che erogano i servizi o realizzano i prodotti) anche con riunioni periodiche svolte ai vari livelli di responsabilità durante le quali vengono

analizzati i risultati delle misure effettuate ed elaborati eventualmente azioni correttive e di miglioramento qualora gli obiettivi di qualità specifici, i metodi e le modalità di trattamento dovessero discostarsi da quanto programmato. Se necessario (in particolare in caso di scostamenti peggiorativi) i contenuti di queste analisi vengono riportati alla direzione.

In base ai risultati della metriche e delle rilevazioni dei livelli di servizio (SLA), riportati in corso d'opera alla Direzione per eccezione, all'andamento economico, all'andamento commerciale, alle azioni correttive e preventive intraprese, ai risultati delle verifiche ispettive, all'adeguatezza dei prodotti, all'analisi dei documenti di registrazione della qualità in generale, la Direzione effettua almeno annualmente il riesame del SGQ riguardante il monitoraggio e l'eventuale ridefinizione degli obiettivi per la qualità e la sicurezza e le performance raggiunte.

Gli obiettivi, elaborati nel dettaglio, sono riportati nel verbale di riesame del SGQ e diffusi al personale.

Tale approccio consente di individuare i processi dell'organizzazione più idonei al raggiungimento degli obiettivi e di programmare in particolare:

- cosa sarà fatto;
- le risorse che saranno richieste fra quelle umane e strumentali, quelle finanziarie e le infrastrutture;
- chi ne sarà responsabile;
- i tempi per il completamento;
- gli indicatori per misurare i progressi nel miglioramento delle prestazioni dell'organizzazione.