Politica del sistema di gestione integrato

Status del Documento

Identificazione

Titolo	Politica del sistema di gestione integrato		
Codice	POL_SGI		
Tipo	Politica		
Revisione	2.2		
N. Pagine	47		
Diffusione	☒Pubblico	☐Riservato	☐Confidenziale
Status	☐In lavorazione	☐Bozza	☒Pubblicato
Owner	RSGSI		

Approvazioni

	Nome e Cognome	Data	Firma
Redatto da	Simone Vagnarelli	2023/11/8	
Verificato da	Roberto Ronzoni	2023/11/8	
Approvato da	Paolo Urbani	2023/11/8	

Revisioni

Data	Rev.	Descrizione Modifica
2020/06/30	1.0	Primo rilascio
2021/11/05	1.1	Aggiornamento attribuzione ruoli RSGSI e ISM
2022/05/11	1.2	Integrazione ISO 27017 e 27018
2023/02/09	2.0	Revisione e aggiornamento ISO 27001:2022
2023/10/31	2.1	Aggiornamento nomina RSI (ISM)
2023/11/8	2.2	Aggiornamento nomina RSGSI

1. Premessa - Generalità - Contesto

Il presente documento stabilisce e identifica in modo chiaro ed esaustivo le "regole" e gli aspetti "fondanti" di LAZIOcrea riguardo l'approccio generale, la filosofia e la politica in relazione alla sicurezza delle informazioni, al sistema di gestione per la qualità, al sistema di gestione dei servizi IT, nonché al sistema di gestione della continuità operativa.
Il codice etico rappresenta l'approccio generale che l'organizzazione, vista come insieme plurale di soggetti, deve tenere in relazione a specifiche tematiche.
La politica del Sistema di Gestione Integrato (di seguito "SGI") rappresenta l'approccio generale di LAZIOcrea rispetto al SGI stesso, alla sua implementazione, al suo mantenimento, alle sue modifiche. La presente politica è l'espressione della volontà dell'Organizzazione di stabilire le regole generali in relazione alla gestione delle informazioni e per un corretto governo del sistema di gestione ai sensi della ISO 27001, della ISO 20000-1, della ISO 22301 e della ISO 9001.
A tal fine si è stabilito di incorporare, nel presente documento, i principi necessari per consentire all'Organizzazione di raggiungere un adeguato livello di compliance alle normative ISO di riferimento.
Ad oggi l'obiettivo di LAZIOcrea non è la certificazione del Sistema di Gestione Integrato, bensì la definizione un di modello di approccio che consenta di cogliere il meglio dalle normative di riferimento mettendo a fattor comune le risorse disponibili e creando nuove sinergie tra le strutture aziendali interessate.
La presente politica si inserisce all'interno di un contesto più ampio, il Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Figura 1 – Sistema documentale del SGSI

2. Benefici del Sistema di Gestione Integrato

LAZIOcrea ha optato per una politica di SGI poiché consapevole che tale approccio porta con sé i seguenti vantaggi:

- *Uniformità di gestione*: la creazione di un unico sistema di gestione aziendale consente modalità uniche per l'organizzazione di tutte le attività legate alla Sicurezza delle Informazioni (ISO 27001), gestione dei Servizi IT (ISO 20000-1), gestione della Qualità (ISO 9001) e della Continuità Operativa (ISO 22301).
- *Ottimizzazione delle risorse*: la gestione uniforme delle tre aree rende possibile lo sfruttamento di sinergie potenziali presenti nell'Organizzazione (es.: audit, formazione, ecc.).
- *Unificazione degli obiettivi di miglioramento*: gli obiettivi principali dell'Organizzazione sono sia di tipo economico che relativi alla soddisfazione dei clienti e delle parti interessate. L'integrazione permette di individuare criteri decisionali univoci per la scelta degli obiettivi aziendali e per la definizione dei programmi per attuarli.
- *Coinvolgimento del personale a tutti i livelli*: la razionalizzazione nell'impiego delle risorse umane e nell'attribuzione delle responsabilità facilita il coinvolgimento e la sensibilizzazione del personale.
- *Semplificazione del rapporto dipendenti/Alta Direzione*: la definizione razionale trasparente di ruoli e responsabilità e la sensibilizzazione dell'impatto che ogni attività può avere sul raggiungimento degli obiettivi fissati, rende più semplici le relazioni tra i diversi livelli dell'organigramma aziendale.
- *Unicità del sistema documentale e della gestione dei dati*: anche a livello di documentazione e modulistica, l'integrazione permette di evitare la duplicazione di registrazioni comuni ai vari ambiti e attraverso la condivisione delle informazioni facilita la comunicazione interna.
- *Individuazione dei nuovi approcci strategici*: l'analisi dei processi dal punto di vista non solo qualitativo ma anche di impatto ambientale e di riduzione dei rischi per i lavoratori, permette di individuare nuovi requisiti, alternative progettuali ed opportunità di risparmio.

3. Metodologia

L'Organizzazione ha sviluppato una metodologia per l'identificazione e la gestione degli obiettivi aziendali, sia generali di tipo strategico, sia per quelli operativi, e quindi identificati come KPI di sistema e/o di processo.
Nella realizzazione del sistema è stata effettuata un'analisi normativa e sono state identificate le leggi e le norme di primaria importanza per la realizzazione del sistema.

L'attuale SGI è conforme alla legge sulla privacy 196/2003 (coordinato ed aggiornato, con le modifiche apportate dalla L. n. 205/2021), alla legislazione italiana sul diritto d'autore e tutela della proprietà intellettuale, alla norma 231/01 ed il regolamento europeo 2016/679 sulla privacy.

Dal punto di vista degli standard, all'interno dell'Organizzazione sono stati utilizzati strumenti specifici per aree ben precise, ovvero:

Conformità avviata e in corso di implementazione:

ISO 9001 per la Qualità
ISO 22301 per la Business Continuity
ISO 27001 per la Sicurezza delle Informazioni
ISO 27017 per la Sicurezza delle Informazioni in cloud
ISO 27018 per la protezione delle PII (Personally Identifiable information) nei servizi di public cloud per i cloud provider
ISO 20000-1 per la Gestione del Servizio

Utilizzate come consultazione e per metodologie

ISO 31000 per il Risk Management
ISO 27005 per il Risk Assessment (come metodologia generale)
ITIL V.4 per la gestione del servizio
COBIT 5 per il governo ICT

Questi ulteriori standard sono stati usati per sviluppare, all'interno del SGI, delle specifiche tematiche.

L'Organizzazione ha impostato la sua struttura in allineamento con il framework ITIL V.4, e da questo ha derivato l'introduzione dei processi di gestione del service Management previsti dalla norma internazionale ISO 20000-1.
LAZIOcrea ritiene che una struttura organizzativa orientata ai processi e "per servizio", con l'apporto dell'applicazione di standard internazionali di riferimento, possa garantire la migliore erogazione dei servizi con i più alti standard di qualità.
L'integrazione organica ed armonica di vari framework e standard internazionali permette di raggiungere l'eccellenza sul servizio, garantendone una opportuna efficacia ed efficienza per rimanere competitivi sul mercato.

Nella progettazione e sviluppo del SGI sono state prese in considerazione tutte le eventuali prescrizioni legali e contrattuali con i clienti. Ciò al fine di garantire anche l'aspetto più squisitamente formale, oltre che quello sostanziale.

3.1. Governo

Le modalità di buona gestione che ci si impegna ad attuare sono, a livello strategico:

- stabilire traguardi ed obiettivi per migliorare continuamente l'efficienza ed efficacia del servizio, attraverso la pianificazione ed il controllo del processo;
- ottimizzazione dell'utilizzo delle risorse umane, finanziarie, infrastrutturali e tecnologiche;
- ricerca di miglioramento delle prestazioni attraverso il monitoraggio della soddisfazione del cliente, la misura dei servizi erogato (SLA o KPI) ed il monitoraggio sistematico dell'operato di tutta l'Organizzazione;
- coinvolgimento, sensibilizzazione ed incremento di consapevolezza e coscienza di tutta l'Organizzazione, promuovendo l'importanza della comunicazione a ogni livello, l'importanza dei controlli come strumenti per migliorare le modalità di progettazione ed erogazione del servizio.

A livello di processi:

- governo e monitoraggio dei processi aziendali significativi, dedicando risorse adeguate e strumenti quali: riesami periodici del sistema da parte dell'Alta Direzione, verifiche ispettive interne, indicatori, riunioni periodiche con tutto il personale;
- garantire l'efficacia del processo attraverso adeguato addestramento del personale, modalità operative definite ed appropriate risorse;
- garanzia della corretta e trasparente gestione del lavoro svolto, sia quando eseguito da personale dipendente, sia quando gestito mediante terzi.

L'attuazione della politica del SGI avviene grazie alla formulazione di obiettivi e di misura dei processi che sono riesaminati almeno una volta all'anno, in fase di riesame della Direzione.

LAZIOcrea pone particolare attenzione al concetto di misura del servizio, che prevede, in fase di progettazione, l'identificazione sia dei KPI sia degli SLA che consentono la massima trasparenza nei confronti del Cliente. Ai fini di un ottimale erogazione dei servizi sono dunque necessari gli indicatori, che permettono il controllo continuo e oggettivo dei livelli di servizio e una comparazione con le tabelle di riferimento, verificando l'andamento del servizio e fornendo eventuali spunti di miglioramento.

4. Glossario - Definizioni

Nel presente documento si utilizza il glossario generale applicato al SGI.
In particolare, sono definiti i seguenti termini, a cui la presente policy si riferisce:

SGI	Sistema di Gestione Integrato (ISO 27001, ISO 20000-1, ISO 22301)
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni (ISO 27001, ISO 27017, ISO 27018)
SGS	Sistema di Gestione del Servizio (ISO 20000-1)
SGCO	Sistema di Gestione per la Continuità Operativa (ISO 22301)
ISM	Information Security Manager / Responsabile della Sicurezza Informatica
RSG	Responsabile del Sistema di Gestione
RSGSI	Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni
Politica	Principi fondamentali e imprescindibili che l'Organizzazione si è data e che devono essere rispettati
DR	Disaster Recovery
BC	Business Continuity
Stakeholder	Portatore di interessi
KPI	Key Performance Indicator
SLA	Service Level Agreement
NDA	Non Disclosure Agreement

5. Riferimenti

Documento	Descrizione
ISO 9001 Quality management systems — Requirements	La ISO 9001 è la normativa di riferimento per il controllo qualità del processo produttivo, la quale in modo ciclico va a definirne tutti gli aspetti, dai requisiti, espressi e non, dei clienti fino al monitoraggio di tutto il percorso/processo produttivo.
ISO 20000-1 Information technology — Service management — Part 1: Service management system requirements	La ISO 20000-1 specifica i requisiti per un'organizzazione al fine di stabilire, implementare e migliorare in modo continuo il sistema di gestione dei servizi.
ISO 22301 Security and resilience — Business continuity management systems — Requirements	Norma internazionale relativa alla gestione della continuità operativa, recepita dall'UNI come UNI EN ISO 22301.
ISO 27001 Information Security Management System	Norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.
ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Norma che fornisce linee guida per i controlli di sicurezza delle informazioni applicabili alla fornitura e all'utilizzo di servizi cloud, con l'implementazione aggiuntiva per i controlli pertinenti specificati nella norma ISO/IEC 27002 e controlli aggiuntivi che riguardano specificamente i servizi cloud.
ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Documento che stabilisce gli obiettivi di controllo, i controlli e le linee guida comunemente accettati per l'implementazione di misure di protezione delle informazioni di identificazione personale (PII) per l'ambiente di cloud computing pubblico.

6. Scopo del documento

Lo scopo della politica generale è quella di identificare le regole fondamentali su cui basare il sistema di gestione integrato e, in generale, tutta l'organizzazione del lavoro.
Questa politica vuole essere lo strumento generale in cui tutti i dipendenti, che sono attivi all'interno dell'Organizzazione, possano trovare la "carta costituzionale" su cui basare processi, procedure, attività, approcci ed altre regole.

7. Campo di applicazione

Si è deciso di includere tutta la struttura operativa all'interno dell'applicazione del sistema, come perimetro logico ed organizzativo.
Il sistema di gestione integrato di LAZIOcrea è applicato in modo verticale e trasversale alle Direzioni Organizzazione, Sistemi Informativi e Sistemi Infrastrutturali.

Tutti i soggetti che operano per il conseguimento degli obiettivi aziendali, siano essi soggetti in posizione apicale, soggetti con funzioni di direzione e rappresentanza, oppure dipendenti, collaboratori e consulenti esterni, fornitori e partner commerciali, sono tenuti, senza eccezione, all'osservanza e condivisione della presente politica nella conduzione delle attività aziendali. L'osservanza della politica deve considerarsi parte essenziale delle obbligazioni contrattuali di tutti i soggetti di cui sopra, destinatari del presente documento secondo quanto stabilito nelle regole aziendali.

8. Valori ed etica aziendale

8.1. Riservatezza e trattamento delle informazioni

L'Organizzazione si impegna a non divulgare, senza specifica autorizzazione scritta, informazioni che riguardano attività ed interessi del Cliente, dei quali sia venuto a conoscenza durante l'espletamento dell'incarico. Tali informazioni vengono coperte da segreto professionale e da clausole specifiche di riservatezza; saranno trattate come riservate anche all'interno dell'Organizzazione. L'Organizzazione non potrà mai utilizzare a vantaggio proprio o di terzi le informazioni di cui potrà venire a conoscenza nel corso dello svolgimento delle proprie attività. L'Organizzazione potrà citare casi aziendali, soluzioni ed esperienze di clienti a terzi, solo avendo rispetto per la riservatezza dei Clienti coinvolti oppure solo su esplicita autorizzazione alla citazione e referenza da parte degli stessi.

Tutti i dipendenti ed i collaboratori, a qualsiasi livello, sono tenuti ad impegnarsi per applicare e fare applicare il principio enunciato sopra.

8.2. Correttezza e trasparenza delle informazioni

Ogni attività, operazione e transazione deve essere correttamente eseguita, registrata, autorizzata, verificabile, rintracciabile, legittima, coerente e congrua. Ciò significa che ciascuna azione ed operazione deve avere una registrazione adeguata nei sistemi aziendali, secondo i criteri indicati dalla legge e dai principi applicabili. Affinché si risponda ai requisiti di verità, completezza e trasparenza del dato ed informazione registrata, ogni operazione deve inoltre essere supportata da idonea documentazione, in modo da consentire in ogni momento all'effettuazione di controlli che ne attestino le caratteristiche e le motivazioni ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

8.3. Comunicazione verso l'esterno

La comunicazione deve essere improntata al rispetto del diritto all'informazione chiara ed esaustiva; in nessun caso è permesso di divulgare notizie o commenti falsi o tendenziosi.
Ogni attività di comunicazione deve rispettare le leggi, le regole, le pratiche di condotta etico-professionale e deve essere realizzata con chiarezza, trasparenza e tempestività.
I rapporti con i mass media sono riservati esclusivamente alle funzioni e alle responsabilità aziendali a ciò delegate.
I dipendenti ed i collaboratori, a qualunque titolo, sono tenuti a dare informazioni complete, trasparenti, comprensibili ed accurate, atte a consentire all'insieme delle parti interessate di giungere, nello sviluppo dei rapporti che vengono instaurati, a decisioni autonome e consapevoli.

8.4. Condotta improntata al coinvolgimento e rispetto

Il dipendente ed il collaboratore devono agire lealmente, nell'osservanza degli obblighi sottoscritti nel contratto di lavoro, di quanto previsto dal Codice Etico e dalle normative aziendali, assicurando elevati standard delle prestazioni rese. Dovrà evitare comportamenti tali da danneggiare gli asset, i servizi, i dati e le informazioni, i beni dell'Organizzazione, la gestione aziendale, il rapporto con le parti interessate e l'immagine aziendale.
Ognuno è un elemento proattivo nella gestione delle attività dal punto di vista dell'analisi degli impatti sull'erogazione del servizio, la sicurezza delle informazioni e sulla continuità operativa. Tutti hanno il dovere, il potere e la possibilità di essere considerati come parte di un sistema complesso; come elementi di un sistema che

interagisce, con l'obiettivo di garantire la continuità operativa dell'Organizzazione e per garantire la salvaguardia delle informazioni.
Le decisioni assunte da ciascuno devono basarsi su principi di sana e prudente gestione, valutando in modo oculato i rischi potenziali, nella consapevolezza che le scelte personali contribuiscono al raggiungimento dei risultati positivi aziendali, ma anche a quelli negativi. Tutte le operazioni e le attività devono essere ispirate alla massima correttezza dal punto di vista della gestione, alla completezza e alla trasparenza delle informazioni, alla legittimità sotto l'aspetto formale e sostanziale e alla chiarezza e verità secondo le norme vigenti.
È fatto obbligo di segnalare all'Organismo di Vigilanza eventuali situazioni anomale o istruzioni ricevute, contrastanti con la legge e le procedure, con la normativa interna o con le regole aziendali, o che possano essere un rischio per la sicurezza e la continuità operativa.

8.5. Rapporti con i clienti

La professionalità, la competenza, la disponibilità, il rispetto e la correttezza rappresentano i principi guida e lo stile di comportamento da seguire nei rapporti con i clienti. Per tutelare l'immagine e la reputazione dell'azienda è indispensabile che i rapporti con i clienti, comprese le comunicazioni, siano improntati:

- al rispetto della legge;
- al rispetto delle regole di base;
- alla piena trasparenza e correttezza;
- all'indipendenza nei confronti di ogni forma di condizionamento, sia interno che esterno;
- alla garanzia di erogazione di qualità dei servizi;
- per la misura dei processi e dei servizi;
- per garantire sicurezza delle informazioni;
- per garantire la continuità del servizio;
- per garantire la corretta gestione della privacy.

8.6. Rapporti con i fornitori

Ogni acquisto in favore della società deve essere condotto con lealtà, integrità, riservatezza, diligenza, professionalità e obiettività di giudizio, da personale qualificato che si assuma la responsabilità delle proprie valutazioni e dei propri giudizi, assicurando nell'attività di acquisto l'osservanza di tutte le disposizioni normative.

Nello specifico, i soggetti responsabili e gli addetti al processo di acquisto devono valutare le seguenti specificità:

- attivano processi di "partnership" in modo da considerare il fornitore come elemento attivo anche nelle scelte strategiche (ove fattibile) e nella piena e proficua collaborazione per entrambi;
- devono attuare un processo di valutazione del rischio, sia del fornitore sia della fornitura;
- identificano i fornitori, i servizi ed i prodotti tali per cui sia garantita una perfetta erogazione di tutti i servizi interni che da questi dipendono;
- identificano le regole, anche ai fini contrattuali, che esplicitino senza ombre le responsabilità ed i ruoli in tutte le fasi di erogazione del prodotto/servizio;
- sono tenuti al rispetto dei principi di imparzialità ed indipendenza nell'esercizio dei compiti e delle funzioni affidate, operando sulla base dell'adozione di criteri oggettivi e documentabili;
- devono mantenere i rapporti e condurre le trattative con i fornitori in modo da creare una solida base per relazioni reciprocamente convenienti e di durata adeguata, nell'interesse della Società;
- sono tenuti tassativamente a segnalare immediatamente all'Alta Direzione qualsiasi tentativo o caso di alterazione dei normali rapporti commerciali;
- non devono offrire beni o servizi, in particolare sotto forma di regali, a personale di altre società o enti per ottenere informazioni riservate o benefici diretti o indiretti rilevanti, per sé o per l'azienda, fermo restando quanto previsto dalle disposizioni generali;
- non devono accettare beni o servizi da soggetti esterni o interni a fronte del rilascio di notizie riservate o dell'avvio di azioni o comportamenti volti a favorire tali soggetti, anche nel caso non vi siano ripercussioni dirette per la Società.

L'Organizzazione promuove sempre e comunque i principi enunciati in queste pagine anche con altri Stakeholder che non siano clienti o fornitori.

8.7. Responsabilità

Tutte le parti interessate dovrebbero assumersi la responsabilità per la gestione del rischio in relazione agli schemi ISO citati, ma non solo.
Tutti devono agire in modo responsabile e tenere conto, sulla base dei loro ruoli e delle loro responsabilità, del contesto e della loro capacità di agire, per la gestione di qualità, continuità e sicurezza del servizio, considerando anche il potenziale impatto delle loro decisioni sugli altri.
Tutti gli attori sono chiamati a riconoscere che un predeterminato livello di qualità, continuità e sicurezza del servizio deve essere assolutamente raggiunto per conseguire gli obiettivi economici, societari, di immagine e di reputazione.

8.8.I diritti umani e i valori fondamentali

Tutte le parti interessate dovrebbero gestire qualità, continuità e sicurezza del servizio in modo trasparente e coerente con i diritti umani e i valori fondamentali della società.
La gestione dei rischi, la qualità, la continuità e la sicurezza del servizio devono essere implementati in un modo che sia coerente con i diritti umani e dei valori fondamentali riconosciuti dalle società democratiche, compresa la libertà di espressione e il libero flusso di informazioni, la riservatezza delle informazioni e la comunicazione, la protezione della privacy e dei dati personali, la trasparenza e l'equità dei trattamenti.
La gestione dei rischi, la qualità, la continuità e la sicurezza del servizio devono essere implementati in modo da essere basati su un comportamento etico che rispetta e riconosce gli interessi legittimi degli altri e di tutta la società.

8.9.Cooperazione

La rete di interconnessione mondiale crea delle interdipendenze tra gli operatori e delle forti motivazioni per la loro cooperazione sul security risk management.
Tutte le parti interessate dovrebbero cooperare, anche al di là dei confini delle proprie attività o sfere di competenza principale.
L'Organizzazione attiva la cooperazione includendo tutte le parti interessate. Ciò ha la sua genesi in seno all'Alta Direzione, per diffondersi in tutte le direzioni, divisioni e le sedi e fra le singole persone.
La cooperazione si estende anche al di là delle frontiere, a livello regionale e a livello nazionale, coinvolgendo tutti gli Stakeholder esterni quali clienti, fornitori, organismi di controllo, associazioni di categoria.

9. Diffusione, disponibilità e riesame della politica

La politica è diffusa e distribuita a tutti i dipendenti e i collaboratori interni ed esterni al fine di comunicare i principi di base del sistema di gestione integrato su:

- gestione e qualità del servizio;
- continuità delle attività;
- sicurezza delle informazioni.

La diffusione della politica aziendale serve in primo luogo ad accrescere la consapevolezza, ovvero arrivare ad "avere coscienza" che un approccio aziendale *è importante*.
Non è detto che sia richiesta una precisa conoscenza di tutti gli aspetti relativi del sistema di gestione e suoi particolari, ma è importante che tutti gli stakeholder

coinvolti nel processo siano consapevoli dell'importanza di una corretta erogazione del servizio, ovvero "di qualità", "in sicurezza", "affidabile" e "totalmente sotto controllo".

La politica del SGI è disponibile a tutto il personale di LAZIOcrea e pubblicata sul sito istituzionale.
L'approccio attivo, interno ed esterno, mediante la diffusione delle politiche a vari livelli, consente di raggiungere gli obiettivi prefissati.

9.1. Riesame della politica

La presente politica viene riesaminata dall'Alta Direzione annualmente o in caso di cambiamenti significativi che influenzano il SGI, al fine di garantirne l'idoneità, l'adeguatezza e l'efficacia.
È responsabilità di tutte le funzioni/strutture osservare il contenuto della presente politica e segnalare al Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) l'esigenza di aggiornare la medesima in funzione di eventuali variazioni che dovessero comportare l'esigenza di modifica delle informazioni in essa contenute (es. variazioni normative, regolamentari, organizzative, operative).

10. Ruoli e responsabilità

L'impegno costante dell'Alta Direzione viene dimostrato attraverso la politica, la fornitura di risorse adeguate a la realizzazione e sviluppo del SGI ed i controlli associati.
L'Alta Direzione garantisce, inoltre, che un riesame sistematico delle prestazioni venga condotto su una base regolare e pianificata, per assicurare che gli obiettivi di gestione siano rispettati e che i problemi siano identificati. Le attività di riesame passano attraverso il programma di audit e l'analisi dei risultati dei processi di gestione.
Nel campo della sicurezza delle informazioni, vi sono un certo numero di ruoli per la gestione, che corrispondono alle aree definite nell'ambito operativo. In una grande organizzazione questi ruoli sono spesso ricoperti da uno o più individui in ogni area, mentre all'interno di una media organizzazione questi ruoli e responsabilità devono essere ripartiti tra i vari membri del team.
I dettagli delle responsabilità associate a ciascuno ruolo e il modo in cui vengono allocate all'interno dell'Organizzazione sono meglio esplicitate all'interno del documento aziendale "Manuale del Sistema per la Gestione per la Sicurezza delle Informazioni" (MSGSI).
È compito di LAZIOcrea assicurare che il personale sia conscio delle proprie responsabilità, e che ognuno abbia le dovute competenze per attuare quanto viene richiesto.

Nei paragrafi seguenti si riportano gli attori tipici del Sistema di Gestione per la Sicurezza delle informazioni, che svolgono ruolo analogo nel Sistema di Gestione Integrato.

10.1. RSGSI - Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni

Il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) ha l'autorità complessiva per assicurare che il Sistema di Gestione per la Sicurezza delle Informazioni sia conforme ai requisiti della norma ISO 27001 e per riferire all'Alta Direzione sulle prestazioni del Sistema.

Il RSGSI è il rappresentante della Direzione e ha la responsabilità complessiva sul Sistema di Gestione per la Sicurezza delle Informazioni. In particolare, si occupa di:

- la definizione della politica di sicurezza del Sistema di Gestione per la Sicurezza delle Informazioni;
- l'identificazione, la documentazione e l'attuazione dei requisiti di sicurezza delle informazioni;
- la progettazione, l'implementazione, la gestione e il miglioramento dei processi di gestione del rischio;
- la gestione e la garanzia dell'integrazione dei processi in ambito di sicurezza ed in particolare di Continuità Operativa e Disaster Recovery;
- di assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme alla norma di riferimento;
- l'identificazione e la gestione della conformità con norme di legge, normative e requisiti contrattuali;
- la promozione della politica di gestione del rischio in tutti i processi aziendali;
- della identificazione, documentazione e attuazione dei requisiti di sicurezza delle informazioni;
- di identificare e gestire la conformità con norme di legge, normative e requisiti contrattuali, compresa la protezione della proprietà intellettuale;
- di riportare all'Alta Direzione la segnalazione per le prestazioni dei processi ed il miglioramento continuo.

L'RSGSI è stato identificato nella persona di Paolo Urbani.

10.2. Responsabile della Sicurezza Informatica (ISM, Information Security Manager)

L'Information Security Manager (ISM) offre le competenze necessarie per verificare e garantire la sicurezza, la qualità e la conformità agli standard tecnologici del sistema informativo interno.

L'ISM è l'autorità complessiva in materia di attuazione e del management dei sistemi di gestione della sicurezza delle informazioni, in particolare si occupa:

- di definire la politica della sicurezza del sistema informativo;
- di valutare i rischi connessi all'uso di specifici strumenti informatici;
- di controllare e supervisionare l'intera infrastruttura tecnologica aziendale per gli aspetti relativi alla sicurezza delle informazioni;
- di assicurare che tutte le informazioni disponibili siano correttamente fruibili, rimanendo al contempo protette da qualsiasi tentativo di accesso non autorizzato;
- del fatto che vengano predisposti adeguati processi di Continuità Operativa e piani di Disaster Recovery;
- dell'integrazione dei processi in ambito di sicurezza ed in particolare di Continuità Operativa e Disaster Recovery.

L'ISM è stato identificato nel ruolo del responsabile della divisione Cyber Security, ruolo ricoperto dal Direttore dei Sistemi Infrastrutturali Vittorio Gallinella.

LAZIOcrea, tenuto conto della propria struttura organizzativa, ha provveduto a individuare specifiche figure deputate, con differenti ruoli e responsabilità, quali responsabili di un servizio, di un processo e di un Asset.

10.3. Risk Manager, Service Owner, Process Owner, Asset Owner, Dipendenti e Collaboratori

Il Risk Manager è colui che governa il processo di gestione del rischio, la cui figura è ricoperta dal RSGSI.
Tale necessità è scaturita dal contesto specifico, in quanto ad oggi non si identificano figure e/o collaboratori che possano ricoprire con efficacia tale responsabilità.

Il Service Owner è il responsabile del servizio erogato al cliente (interno o esterno) e svolge le seguenti attività:

- rappresenta il servizio all'interno dell'Organizzazione, a prescindere da dove siano fisicamente collocati gli strumenti per erogarlo;
- interagisce con i clienti, con gli altri Service Owner e con i Process Owner;
- è responsabile dell'erogazione dei servizi secondo gli SLA e gli OLA;
- collabora all'individuazione della causa ultima in un incidente e rappresenta il servizio nel CAB (Change Advisory Board).

Il Process Owner è il responsabile del processo affinché venga eseguito nel rispetto degli standard fissati; si occupa della gestione e del supporto quotidiano al processo; definisce le metriche del processo.

L'Asset Owner è il responsabile dell'asset all'interno dell'Organizzazione; si occupa della gestione e verifica del corretto funzionamento ed utilizzo dell'asset di riferimento nonché del supporto ordinario e straordinario al servizio e agli attori di interessati. Nel fare questo è supportato dagli operatori incaricati di intervenire sugli asset nelle attività quotidiane.

Dipendenti e collaboratori sono responsabili della sicurezza delle informazioni e rientra nelle loro mansioni il dovere di attuare la politica per la sicurezza delle informazioni, affinché vi sia un miglioramento della stessa.
Ad esempio, dovrebbero segnalare, al Responsabile della Sicurezza delle Informazioni, potenziali punti deboli o violazioni riguardanti la sicurezza delle informazioni.
La stessa sensibilizzazione è estesa ai fornitori e al personale esterno che supporta il personale e le attività di LAZIOcrea.

11. Normative

La Politica del Sistema di Gestione Integrato nasce affinché LAZIOcrea possa ritenersi ragionevolmente conforme alle normative ISO di riferimento, adottando le best practices di riferimento e rispettando i requisiti contenuti all'interno degli stessi standard ISO.
Gli standard ISO oggetto della presente politica sono i seguenti:

- ISO 9001:2015 Sistema di Gestione della Qualità;
- ISO 20000-1:2018 Sistema di Gestione dei Servizi IT;
- ISO 27001:2022 Sistema di gestione della Sicurezza delle Informazioni;
- ISO 22301: 2019 Sistema di Gestione della Continuità Operativa;
- ISO/IEC 27017:2015 Codice per la sicurezza delle informazioni dei servizi cloud;
- ISO/IEC 27018:2019 Codice per la protezione dei dati personali dei servizi cloud.

Il presente documento rappresenta la volontà dell'Organizzazione di stabilire le regole generali per un corretto governo del sistema di gestione ai sensi delle norme ISO sopra citate; a tal fine il documento accorpa al suo interno i segni distintivi di ciascuna norma e riporta gli elementi comuni degli standard ISO, al fine evitare ridondanze.

La politica generale del sistema integrato tratta gli elementi generali di ciascuno standard, definendone lo scopo e tratti distintivi, con il fine di rendere partecipe

l'intera Organizzazione riguardo gli obiettivi da perseguire e le modalità attraverso le quali è possibile raggiungere gli obiettivi stessi.
Si evince, pertanto, che questa politica non è un manuale attraverso la cui applicazione si raggiunge la perfetta conformità agli standard ISO di riferimento: per tale fine, ovvero per il dettaglio e l'applicazione dei controlli, si rimanda agli standard stessi, alle politiche specifiche e alle procedure/istruzioni operative di LAZIOcrea.

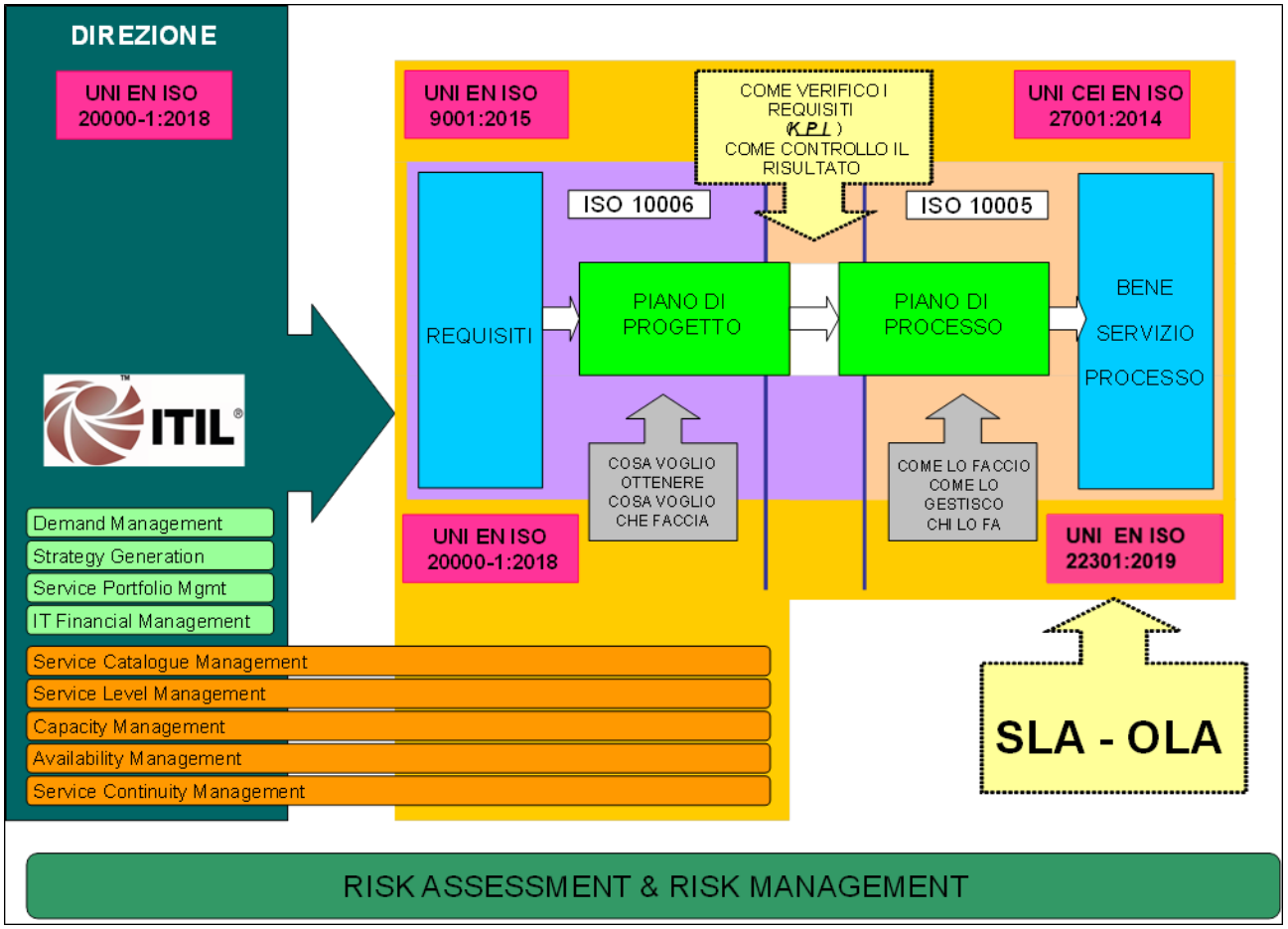

Figura 2 – Relazione tra normative

Nei paragrafi successivi verranno descritti, per ciascun ambito di applicazione del SGI, lo scopo, i principi, i concetti chiave, gli obiettivi e i vantaggi.

11.1. ISO 9001 Sistema di Gestione per la Qualità

La ISO 9001 è la norma internazionale per i Sistemi di Gestione per la Qualità (SGQ), pubblicata dall'ISO (International Organization for Standardization).

È lo standard di riferimento internazionalmente riconosciuto per la gestione della Qualità di qualsiasi organizzazione che intenda rispondere contemporaneamente:

- all'esigenza dell'aumento dell'efficacia ed efficienza dei processi interni , quale strumento di organizzazione per raggiungere i propri obiettivi;
- alla crescente competitività nei mercati attraverso il miglioramento della soddisfazione e della fidelizzazione dei clienti.

Il Sistema di Gestione per la Qualità è una raccolta di politiche, processi, procedure documentate e registrazioni. Questo insieme di documenti definisce le regole interne che definiscono il modo in cui LAZIOcrea fornisce il prodotto o il servizio ai clienti.

11.2. Scopo della norma

In quanto norma internazionale, la ISO 9001 è riconosciuta come base per creare un sistema che assicuri la soddisfazione del cliente e il miglioramento continuo.
Lo scopo primario dell'ISO 9001 è il perseguimento della soddisfazione del proprio cliente in merito ai prodotti e servizi forniti, nonché il miglioramento continuo delle prestazioni aziendali, permettendo all'Organizzazione certificata di assicurare ai propri clienti il mantenimento e il miglioramento nel tempo della qualità dei propri beni e servizi.

Da questo punto di vista il modello ISO 9001 rappresenta uno strumento strategico in quanto mirato a:

- valutazione del contesto e parti interessate;
- analisi di rischi ed opportunità come base per definire opportune azioni;
- controllo dei costi;
- aumento della produttività;
- riduzione degli sprechi.

11.3. Principi

Nello specifico delle tematiche per la Qualità, LAZIOcrea si impegna a svolgere le proprie attività secondo la norma UNI EN ISO 9001, attraverso i seguenti principi:

- mantenere adeguata la qualità delle prestazioni, in particolare garantendo l'efficienza, la continuità e sicurezza del servizio nel rispetto dei requisiti richiesti (cogenti e non) per l'erogazione del servizio;
- mantenere adeguati i servizi offerti ai clienti;

- rispettare tempi di consegna ed ottimizzare il rapporto costo/qualità dei servizi;
- proporre e consuntivare annualmente piani di miglioramento per tutto il Sistema di Gestione Integrato, rendendo visibili i risultati a tutta l'Organizzazione tramite la pubblicazione del riesame all'interno del sistema documentale;
- monitorare e revisionare i sistemi di gestione, attraverso puntuali piani di consuntivazione e miglioramento.

11.4.Concetti chiave

La ISO 9001 pone al centro della realizzazione di un sistema di gestione:

- il cliente e la sua piena soddisfazione;
- lo studio del contesto e conseguenti rischi ed opportunità imprenditoriali;
- la visione dell'azienda come un insieme di processi tra loro in stretta relazione e finalizzati a fornire prodotti che rispondano in modo costante ai requisiti fissati;
- l'importanza di perseguire il continuo miglioramento delle prestazioni.

Gestire la qualità significa gestire consapevolmente l'efficacia e l'efficienza dei propri processi attraverso:

- la conoscenza, la gestione e il monitoraggio dei processi;
- la capacità di coinvolgere le risorse umane;
- la centralità del ruolo dell'Alta Direzione aziendale;
- la capacità di misurare le proprie prestazioni ed il grado di raggiungimento degli obiettivi.

11.5. Obiettivi

Gli obiettivi strategici del SGQ, che interagiscono tra loro in modo sinergico, sono:

- assicurare che i bisogni dei clienti siano definiti e soddisfatti allo scopo di accrescerne la soddisfazione (Customer Satisfaction) e incrementare la loro fidelizzazione;
- aumentare la comprensione e la motivazione del personale verso i traguardi e gli obiettivi aziendali, ed il loro apporto al miglioramento continuo dell'Organizzazione (Employee Satisfaction);
- migliorare la professionalità del personale e il suo utilizzo in modo efficace ed efficiente;

- incrementare il vantaggio competitivo dell'azienda in modo efficace ed efficiente migliorando i risultati operativi e le quote di mercato;
- sviluppare la capacità di creare valore sia attraverso l'ottimizzazione dei costi e delle risorse che aumentando la velocità di risposta al mercato;
- per rendere sistematici la pianificazione ed il raggiungimento di tali obiettivi e per renderli visibili ai propri Clienti, l'Alta Direzione oltre ad assicurare il proprio supporto, l'impiego di tutte le risorse finanziarie e professionali necessarie, intende fornire strumenti ed azioni volte a favorire la piena adozione del sistema di gestione per la qualità da parte di tutte le persone coinvolte nell'Organizzazione ed incentivare il contributo di ognuno al suo miglioramento continuo.

11.6.Benefici

I vantaggi derivanti dall'applicazione della norma sono i seguenti:

- rendere sistematica la valutazione di rischi ed opportunità su cui basare decisioni strategiche;
- adozione di un modello organizzativo basato sull'approccio integrato ai processi e sulla condivisione delle esperienze dei singoli per migliorare in modo efficace e continuo le prestazioni;
- accrescere la capacità di soddisfare le esigenze e le aspettative dei propri clienti attraverso una migliore conoscenza e controllo dell'azienda;
- diminuzione dei costi connessi all'inefficienza delle attività svolte;
- puntuale definizione delle responsabilità e di percorsi di crescita professionale delle risorse impiegate;
- trasparenza verso i mercati di riferimento.

11.7.20000-1 Sistema di Gestione dei Servizi

La norma ISO 20000-1 stabilisce lo standard per la gestione ed il controllo di servizi IT.
L'ISO 20000-1 contiene i requisiti normativi e una lista di controlli a cui una organizzazione deve aderire per fornire dei servizi di gestione della qualità accettabili per i suoi clienti.
In tal senso la norma ISO 20000-1 costituisce lo strumento adeguato sia per la gestione dei servizi erogati ai clienti, sia per la gestione dei servizi informatici interni che necessitino di un livello di strutturazione consistente.

11.8.Scopo della norma

La norma mira al miglioramento dell'erogazione/fruizione dei servizi IT, ponendosi come obiettivo il raggiungimento della massima qualità dei servizi erogati e un massimo contenimento di costi.
L'Alta Direzione di LAZIOcrea è convinta che il processo di miglioramento continuo costituisca l'elemento fondamentale per raggiungere l'eccellenza nel coniugare la crescita aziendale con elevati standard di qualità ed efficienza dei servizi erogati.

I modelli adottati da LAZIOcrea assegnano al cliente un ruolo primario: la piena comprensione delle esigenze e la progettazione di soluzioni personalizzate garantiscono il raggiungimento di obiettivi di eccellenza.

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

11.9. Principi

LAZIOcrea si impegna a svolgere le proprie attività secondo la norma UNI EN ISO 20000-1, attraverso il rispetto dei seguenti principi:

- stabilire e comunicare il campo di applicazione, la politica e gli obiettivi relativi alla gestione del servizio;
- assicurare che siano eseguite attività per identificare, documentare e soddisfare i requisiti dei prodotti e dei servizi;
- assicurare, in tutta l'Organizzazione, la promozione della consapevolezza dell'importanza di soddisfare sempre i requisiti dei clienti e quelli regolamentari;
- assicurare che i beni, comprese le licenze, usate per sviluppare i prodotti ed erogare i servizi, siano gestiti secondo le prescrizioni legali e regolamentari nonché gli obblighi contrattuali;
- assicurare che, per ogni servizio erogato sia creato, attuato e mantenuto aggiornato un piano di gestione del servizio al fine di adempiere alla politica, conseguire gli obiettivi per la gestione del servizio e soddisfare i requisiti del servizio;
- comunicare l'importanza di soddisfare i requisiti del servizio, promuovendo in tutta l'Organizzazione la consapevolezza dell'importanza di soddisfare sempre i requisiti dei clienti e quelli regolamentari;

- comunicare l'importanza di soddisfare le prescrizioni legali e regolamentari, nonché gli obblighi contrattuali;
- assicurare la messa a disposizione di risorse;
- condurre i riesami di direzione ad intervalli prestabiliti;
- assicurare che i rischi per i servizi siano valutati e gestiti;
- assicurare che siano definite e tenute aggiornate le autorità e responsabilità per la gestione del servizio;
- assicurare che siano eseguite attività per identificare, documentare e soddisfare i requisiti dei prodotti e dei servizi;
- assicurare che i beni, comprese le licenze, usate per sviluppare i prodotti ed erogare i servizi, siano gestiti secondo le prescrizioni legali e regolamentari nonché gli obblighi contrattuali.

11.10. Concetti chiave

Gli elementi di rilievo della norma sono i seguenti:

- Controllo e misura del servizio: nella definizione dei servizi, grande impegno è profuso per identificare sia i sistemi che le modalità per una misura del servizio, in diverse forme e gradi di approfondimento.

La struttura del servizio prevede, in fase di progettazione, l'identificazione sia dei KPI sia degli SLA che saranno componente fondamentale per la massima trasparenza nei confronti del Cliente. L'Organizzazione crede fermamente che per l'erogazione del servizio sia vitale il recupero di dati, statistiche ed indicatori tali per cui:

- i dati siano coerenti e congrui, e raccolti nella giusta quantità;
- i dati e le informazioni siano fruibili e utilizzabili per la gestione del servizio;
- gli indicatori consentano il controllo continuo e oggettivo dei livelli di servizio;
- la struttura informativa, di controllo e tutti gli indicatori, permettano di attivare i processi di miglioramento continuo sia delle prestazioni sia dell'efficienza del binomio "struttura – servizio".

Tutti i collaboratori, ed in generale gli Stakeholder, sono parte attiva nel processo di misura e controllo.

- Orientamento al cliente: LAZIOcrea dipende dai propri clienti e pertanto cerca di soddisfare le loro esigenze presenti e future, soddisfare i loro requisiti e mirare a superare le loro stesse aspettative.

- Coinvolgimento del personale: LAZIOcrea è consapevole che le persone, a tutti i livelli, costituiscono l'essenza dell'Organizzazione ed il loro pieno coinvolgimento permette di porre le loro capacità al servizio dell'Organizzazione.
- Chiara definizione dei ruoli e responsabilità: LAZIOcrea definisce in modo chiaro le responsabilità del personale e degli utenti in relazione ai requisiti dei propri sistemi di gestione.
- Trasparenza: LAZIOcrea definisce e rende pubblici i propri principi etici e di comportamento mediante la pubblicazione del "Codice Etico".
- Approccio per processi: LAZIOcrea favorisce un approccio per processi al fine di perseguire i risultati desiderati con maggior efficienza.
- Miglioramento continuo: il miglioramento continuo delle prestazioni complessive sono un obiettivo permanente di LAZIOcrea.
- Rapporti di reciproco beneficio con i fornitori: LAZIOcrea ed i suoi fornitori sono interdipendenti, ed un rapporto di reciproco beneficio migliora, per entrambi, la capacità di creare valore.

11.11. Obiettivi

L'obiettivo primario del Sistema di Gestione dei Servizi è migliorare, in modo sistematico, l'erogazione dei servizi. Tale scopo può essere raggiunto attraverso il perseguimento dei seguenti obiettivi:

- stabilire un rapporto di collaborazione e fiducia con i fornitori, atto a raggiungere l'obiettivo comune di erogare servizi e prodotti che soddisfino le esigenze del cliente;
- aumentare le competenze, il coinvolgimento e la consapevolezza del personale, ottimizzandone così anche l'impiego;
- definire, mantenere e migliorare il catalogo dei servizi in aderenza alle esigenze dei propri clienti, progettando e fornendo servizi idonei e innovativi e che creino per loro sempre maggior valore;
- garantire ai propri clienti la costante disponibilità di persone, processi e tecnologie a supporto dei servizi erogati e nel rispetto dei livelli di servizio definiti (SLA);
- assicurare che LAZIOcrea possa continuare le attività di business anche in caso di situazioni avverse;
- definire, attuare e monitorare gli obiettivi per quanto riguarda i piani di gestione del servizio, di continuità, di disponibilità, di capacità e di rilascio/messa in funzione, così come previsto dalla norma in riferimento;
- assicurare il miglioramento continuo dei servizi, processi, risorse, capacità per garantire l'efficacia e l'efficienza presente in un mercato competitivo;

- sviluppare accordi, partnership con fornitori e terze parti, allo scopo di garantire un catalogo servizi più ampio e una maggiore competitività finalizzata alla soddisfazione del cliente e delle parti interessate.

11.12. Benefici

La conformità allo standard ISO/IEC 20000-1 consente a LAZIOcrea di erogare i servizi in modo vantaggioso verso i propri clienti, garantendo sistematicamente il rispetto degli SLA (Service Level Agreement) concordati. In particolare, i benefici sono:

- Realizzazione di un Sistema di Gestione dei Servizi utile al miglioramento continuo della propria attività. Lo standard aggiornato garantirà che la gestione dei servizi sia integrata ed allineata con le strategie aziendali dell'Organizzazione. Questo orientamento strategico consentirà di ottimizzare le prestazioni del Sistema di Gestione dei Servizi (SMS), rendendolo più efficace per tutte le parti interessate.
- Leadership. Un maggiore coinvolgimento del team nel Sistema di Gestione da parte della leadership garantirà all'intera Organizzazione di comprendere i requisiti di Gestione dei Servizi, motivando così l'intero team per il raggiungimento dei propri obiettivi e di quelli dell'Organizzazione.
- Maggiore attenzione alla domanda e alla comprensione. Incorporare domanda e conoscenza è una novità dello standard che può essere applicato alla Gestione dei Servizi dell'intera Organizzazione oltre a quello specifico dell'IT.
- Chiarezza nella gestione dei fornitori. Parametri chiari sulla gestione dei fornitori aiutano ad integrare approcci più efficaci per migliorare le relazioni e l'efficienza di tutti i soggetti coinvolti.

11.13. 22301 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa

ISO 22301 è lo standard del Sistema di Gestione della Continuità Operativa (SGCO) che aiuta le organizzazioni a prepararsi ad affrontare le interruzioni di operatività a causa di eventi avversi.

La Norma ISO 22301 stabilisce i requisiti per un efficiente Sistema di Gestione per la Continuità Operativa. Si tratta di una metodologia costituita da un insieme di prassi volte al mantenimento della Continuità Operativa sotto avverse condizioni, minimizzando l'impatto di potenziali incidenti su clienti, stakeholder e sull'intero "sistema aziendale".

La norma specifica i requisiti per attuare, mantenere e migliorare un sistema di gestione per proteggere l'Organizzazione, ridurre la probabilità che si verifichino, prepararsi, rispondere e riprendersi dalle interruzioni quando si verificano, cioè un efficace sistema di gestione per la continuità operativa.

La ISO 22301 sancisce l'importanza dei piani di Continuità Operativa rispetto al Disaster Recovery: il Disaster Recovery interviene a seguito dell'evento e della sua stabilizzazione (es. restore con backup), mentre la Business Continuity agisce anche sugli aspetti preventivi e di risposta tempestiva all'evento, ad esempio attraverso Business Impact Analysis, Business Continuity Plan specifici.

11.14. Scopo della norma

La norma ISO 22301 è finalizzata a fornire un approccio sistemico per la predisposizione di un piano di prevenzione e di emergenza, in caso di situazioni critiche che mettono a repentaglio il business.
Basandosi sulla messa in atto di varie best practices, lo standard aiuta a comprendere, sviluppare e implementare un SGCO strutturato, preparandosi ai rischi e riducendoli al minimo, rispondendo in modo adeguato a ripristinare l'operatività nel più breve tempo possibile qualora si verifichi un evento che provochi l'interruzione dell'operatività.
La conformità a tale norma rappresenta un attestato di qualità, anche verso l'esterno, perché dimostra la capacità dell'Organizzazione di rispondere rapidamente a blocchi operativi, continuando a fornire il servizio richiesto durante episodi gravosi.

LAZIOcrea ha scelto di uniformarsi alla norma poiché ha la necessità di:

- attuare, mantenere e migliore il proprio SGCO;
- garantire la conformità con la politica di continuità operativa dichiarata;
- essere in grado di continuare a fornire servizi ad una capacità predefinita accettabile durante un'interruzione;
- migliorare la propria resilienza attraverso l'effettiva applicazione del SGCO.

11.15. Principi

LAZIOcrea si impegna a svolgere le proprie attività secondo la norma UNI EN ISO 22301, attraverso il rispetto dei seguenti principi:

- comprendere le esigenze dell'Organizzazione e le necessità per stabilire la politica e gli obiettivi per la continuità operativa;

- gestire e mantenere processi, capacità e strutture di risposta per garantire che l'Organizzazione sopravviva a interruzioni;
- implementare e rendere operativi controlli e misure per gestire la capacità di un'intera Organizzazione nella gestione delle interruzioni (discontinuità) dell'operatività dovute a cause accidentali;
- monitorare e riesaminare le prestazioni e l'efficacia del sistema di gestione della continuità operativa; migliorare in modo continuo il SGCO basato su metriche qualitative e quantitative (obiettivi misurabili).

11.16. Concetti Chiave

Gli elementi di rilievo della norma sono i seguenti:
Resilienza Organizzativa: la norma ISO 22301 riguarda la costruzione e il continuo miglioramento del livello di resilienza del business. Per resilienza organizzativa si intende la capacità di un'organizzazione di anticipare, prepararsi, rispondere e adattarsi al cambiamento graduale e a inconvenienti improvvisi, con l'obiettivo di sopravvivere e prosperare."

Continuità Operativa: la continuità operativa è l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale. Prevenire le interruzioni e avere in atto un buon piano d'emergenza risulta quindi essenziale per mantenere la Continuità Operativa del business sotto le condizioni più avverse.
Nella continuità operativa l'Organizzazione evidenzia il massimo grado di impegno dell'erogazione dei servizi.
Il sistema di gestione della continuità operativa è un "valore" aziendale che porta benefici a tutti gli attori coinvolti nell'erogazione dei servizi, dal fornitore al cliente, con la partecipazione attiva di tutti gli Stakeholder coinvolti.
La struttura ed il sistema di continuità operativa di LAZIOcrea sono in corso di disegno, usando tutte le competenze del personale a tutti i livelli; la progettazione del sistema è stata un lavoro corale in quanto tutti sono stati elementi attivi nella definizione del sistema.

Piano di Continuità Operativa: (di seguito indicato con l'acronimo BCP) è l'insieme di procedure che guidano l'Organizzazione nel rispondere ad un evento avverso che possa degradare o compromettere l'erogazione dei servizi informativi, nel contenere gli effetti dell'evento sui propri asset, e nel ripristinare e mantenere a un livello predefinito ed accettabile i processi di missione.
Il Piano di Continuità Operativa è predisposto in accordo alle strategie definite dal processo di gestione della Continuità Operativa e alle procedure di emergenza di cui già dispone l'Organizzazione.

Business Impact Analysis: (BIA, Analisi degli Impatti sul Business) è una metodologia di analisi che consente di determinare l'impatto e le ricadute sul business aziendale di eventi che causano l'interruzione della produzione o dell'erogazione di servizi.
Tale analisi consente di stabilire le priorità per il recupero dei processi critici.

Stakenholders (o parti interessate): per questa norma il concetto di "parti interessate" o stakeholders è molto importante in quanto una discontinuità (interruzione) nell'operatività dell'Organizzazione, una indisponibilità dei servizi essenziali per i clienti, un fermo delle attività produttive per un periodo più o meno lungo, possono causare danni, sia dal punto di vista commerciale, sia da quello finanziario, ma anche da quello delle altre parti interessate, quali personale interno, individui della collettività che subiscono danni anche fisici, fornitori, ecc.

11.17. Obiettivi

Di seguito vengono riportati alcuni obiettivi di continuità operativa atti a soddisfare i requisiti della ISO 22301:

- riduzione della probabilità di accadimento di eventi negativi;
- aumento dei livelli di risposta e ripristino dell'operatività nel più breve tempo possibile qualora si verifiche un evento che provoca l'interruzione dell'operatività;
- riduzione dell'impatto economico di incidenti, interruzioni e disastri;
- migliore reputazione attraverso la dimostrazione di un approccio professionale in merito alla gestione di un'interruzione come certificato da un sistema;
- facilitazione nei processi di fornitura.

11.18. Benefici

La conformità allo standard ISO 22301 consolida la resilienza dell'Organizzazione e garantisce una maggiore efficienza dei tempi di ripristino, oltre a comportare ulteriori vantaggi, quali:

- identificazione e gestione delle minacce attuali e future dell'Organizzazione;
- approccio proattivo per ridurre al minimo l'impatto degli incidenti;
- mantenimento dell'attività delle funzioni critiche durante i periodi di crisi;
- riduzione al minimo dei tempi di inattività durante gli incidenti e miglioramento dei tempi di recupero;
- miglioramento delle performance, anche in caso di eventi o situazioni che limitano l'operatività;

- riduzione dell'esposizione legale e finanziaria grazie ad un consolidato Business Continuity Plan (BCP);
- maggior vantaggio competitivo;
- maggiore garanzia di affidabilità e stabilità ai clienti, garantendo tempi e modi per le forniture nel caso di interruzioni nell'operatività;
- maggiore capacità di protezione degli asset aziendali;
- salvaguardia dell'immagine e della reputazione aziendale e degli interessi degli stakeholders;
- riduzione di costi derivanti da un'incidente di discontinuità;
- riduzione dei premi assicurativi;
- contributo alla propria resilienza organizzativa.

11.19. ISO 27001
11.20. Scopo della norma

L'obiettivo dello standard ISO 27001 è quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato Sistema di Gestione della Sicurezza delle Informazioni (SGSI) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.

Consapevole del fatto che le proprie attività di progettazione e sviluppo/erogazione per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, LAZIOcrea opera secondo normative di sicurezza internazionalmente riconosciute.
In particolare, per la componente Cloud Computing, LAZIOcrea ha stabilito di implementare il Sistema di Gestione per la Sicurezza delle Informazioni attraverso l'adozione delle norme ISO 27017 e ISO 27018 rispettivamente per i controlli di sicurezza generali per gli utilizzatori e i fornitori di servizi cloud e per i controlli per i fornitori di servizi cloud pubblici che agiscono come responsabili del trattamento.

Su tale linea LAZIOcrea ha deciso di attuare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme ai requisiti della norma internazionale ISO/IEC 27001.

11.21. Principi

Nello specifico ambito delle tematiche per la Sicurezza delle Informazioni, LAZIOcrea si impegna inoltre a svolgere le proprie attività secondo la norma ISO/IEC 27001 e nel rispetto delle migliori best practices e dei principi più avanzati di cyber-security, attraverso i seguenti principi:

- sviluppare, mantenere e migliorare il quadro normativo interno fondato su una politica per la Sicurezza delle Informazione a due livelli (indirizzi strategici e politiche specifiche), che delinea il modello di "governance" e stabilisce ruoli, responsabilità, framework ed altri strumenti di supporto, tra cui standard e metodologie;
- ripartire ruoli e responsabilità nella gestione della sicurezza delle informazioni dei servizi cloud;
- predisporre tutte le azioni necessarie per perseguire obiettivi di sicurezza congrui con il grado di sensibilità delle Informazioni aziendali e di criticità delle tecnologie che consentono il loro trattamento, attraverso la tutela degli attributi di:
  - Riservatezza, mediante interventi idonei a contrastare accessi non autorizzati alle Informazioni o la diffusione o divulgazione non controllate delle stesse;
  - Integrità, mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate, compresi gli errori umani, o il danneggiamento del formato fisico e/o del contenuto semantico delle Informazioni;
  - Disponibilità, mediante interventi idonei a garantire l'accesso alle risorse informative con tempi e modalità "congrue" con le esigenze delle attività di business;

- effettuare sistematicamente attività di analisi e gestione del rischio in funzione della classificazione di sicurezza delle informazioni, in conformità alle politiche ed ai modelli aziendali, per identificare i controlli necessari;
- integrare la sicurezza all'interno del ciclo di vita dei progetti ICT, implementando sui componenti ICT dei Sistemi Informativi aziendali (server, computer desktop e laptop, infrastrutture, applicazioni, database, reti informatiche, ecc.) le misure di protezione funzionali ad una corretta postura di sicurezza;
- garantire nel tempo la conformità dei Sistemi Informativi agli standard di sicurezza aziendali;
- monitorare a livello aziendale lo stato della sicurezza delle informazioni e dei sistemi ICT e il livello di compliance al quadro normativo interno ed agli eventuali vincoli di legge;
- prevenire e gestire gli eventi e/o gli incidenti di sicurezza delle informazioni, raccogliendo e conservando le relative registrazioni, anche ai fini di analisi forensi e programmi di miglioramento;
- osservare con continuità l'evoluzione del quadro esterno di minacce di natura "cyber" e ne trae elementi per aggiornare i programmi di difesa;
- promuovere ed attuare i piani mirati o diffusi di formazione e sensibilizzazione sulla sicurezza delle informazioni;

- interagire con le istituzioni deputate per contribuire al piano nazionale per la protezione cibernetica e la sicurezza informatica, per il potenziamento della capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il Paese.

11.22. Concetti chiave

Gli elementi di rilievo della norma sono i seguenti:

- L'informazione come bene da preservare. L'informazione è un bene fondamentale. Il sistema informativo, ed in particolare quello informatico, sono la spina dorsale su cui si basa l'infrastruttura e l'erogazione stessa dei servizi verso tutti i clienti, sia interni che esterni.

L'informazione è una risorsa che deve essere preservata anche in funzione di specifici obblighi contrattuali.
Preservare l'integrità dell'informazione e dei dati è una priorità di primo livello per LAZIOcrea, anche al fine di garantire la continuità del servizio.
La perdita, la corruzione, la modifica non consentita, l'indisponibilità, la diffusione non regolamentata, il furto, e l'utilizzo illecito dei dati e delle informazioni sono potenzialmente distruttivi: questo sia in modo diretto, sia indiretto.
Trattamento dell'informazione e dei dati. L'informazione deve essere trattata il meno possibile. Nel Testo Unico della Privacy è presente un principio di base fondamentale, ovvero che il trattamento deve avvenire riducendo al minimo l'utilizzo di dati.
Di conseguenza le regole sono:

- principio di necessità;
- liceità e correttezza del trattamento;
- finalità specifiche del trattamento;
- esattezza e aggiornamento dei dati;
- pertinenza, completezza e non eccedenza dei dati raccolti, rispetto alle finalità del trattamento;
- conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento.

I principi che la legge impone per il trattamento dei dati personali sono estendibili anche a qualsiasi tipo di informazione o dati trattati all'interno dell'Organizzazione.

- Sicurezza delle informazioni: per sistema aziendale di sicurezza informatica si intende: l'insieme delle misure tecniche e organizzative volte ad assicurare

la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

La sicurezza delle informazioni è caratterizzabile come salvaguardia di:

- Riservatezza: garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate;
- Integrità salvaguardia dell'accuratezza e della completezza dell'informazione);
- Disponibilità assicurazione che gli utenti autorizzati abbiano accesso alle informazioni ed alle risorse associate quando ne hanno bisogno).

.

- Riservatezza: è la garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla.

La memorizzazione non controllata o gestita, e di pari passo la trasmissione o diffusione di una informazione non autorizzata, viene considerata una violazione della riservatezza, anche se la stessa non viene conosciuta, ricevuta, percepita o interpretata da una persona o da un sistema elettronico.

- Integrità: è la garanzia che ogni informazione sia realmente quella originariamente immessa nel sistema informativo e che il dato sia stato eventualmente modificato esclusivamente in modo legittimo ed in forma

controllata. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati o da sistemi automatici anche come elemento "slegato" da un soggetto specifico.

- Disponibilità: è la garanzia di reperibilità di informazioni in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

La gestione e il miglioramento della sicurezza informativa fanno parte di un processo continuo che deve tenere conto di molteplici fattori di resistenza, interni ed esterni all'azienda, e che deve ricercare costantemente il miglior compromesso tra sicurezza e fruibilità del sistema.

11.23. Obiettivi

L'Alta Direzione ha stabilito i seguenti obiettivi per la Sicurezza delle Informazioni:

- stabilire ed attuare un Sistema di Gestione per la Sicurezza delle Informazioni sulla base della norma ISO/IEC 27001;
- garantire un appropriato livello di sicurezza delle informazioni nell'ambito del ciclo di vita dei prodotti e dei servizi erogati alla propria clientela, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i prodotti/servizi stessi sono soggetti;
- assicurare la continuità dei processi di business aziendali e dei servizi erogati ai propri Clienti interni e del Cloud;
- prevenire gli incidenti della sicurezza delle informazioni e minimizzarne gli impatti, salvaguardando gli interessi aziendali e delle altre parti interessate;
- assicurare la conformità alla normativa cogente applicabile;
- aumentare, nel proprio personale, il livello di consapevolezza e la competenza sui temi della sicurezza delle informazioni;
- salvaguardare l'immagine aziendale percepita dai clienti, quale fornitore affidabile e competente;
- identificare opportunità di miglioramento finalizzate ad aumentare l'efficacia e l'efficienza del sistema di gestione e dei suoi processi.

11.24. Benefici

I vantaggi derivanti dall'applicazione della norma sono i seguenti:

- adozione di Best Practices globalmente accettate;
- adozione di un linguaggio comune e strutturato per la sicurezza delle informazioni che permetta una maggiore fiducia da parte dei clienti;

- maggiore fiducia degli stakeholders;
- garanzia dell'identificazione, valutazione e gestione dei rischi attraverso la corretta valutazione del contesto e l'introduzione delle migliori prassi per il trattamento del rischio stesso;
- aumento della resistenza agli attacchi informatici: un SGSI è in grado di adattarsi ai cambiamenti interni ed esterni all'Organizzazione, in modo tale da prendere in considerazione minacce nuove o mutate;
- soddisfacimento dei bisogni e delle aspettative societarie;
- riduzione dei costi della sicurezza delle informazioni: il SGSI basato sulla valutazione del rischio, ossia sui rischi reali che influenzano gli aspetti dell'Organizzazione, consente di allocare il budget per la sicurezza in modo più efficiente e ridurre i costi per la sicurezza superflui;
- vantaggio competitivo soddisfacendo i requisiti contrattuali dei propri clienti, con particolare attenzione alla sicurezza delle loro informazioni;
- supporto all'Organizzazione a formulare i propri obiettivi e requisiti di sicurezza, fornendo allo stesso tempo una struttura che aiuti a raggiungere tali obiettivi e a rispettare tali requisiti prefissati;
- sostegno al rispetto dei requisiti cogenti;
- protezione delle informazioni aziendali, consentendo di preservare la disponibilità, la riservatezza e l'integrità delle informazioni;
- miglioramento della cultura aziendale: l'approccio dello standard copre l'intera Organizzazione aziendale, non solamente l'ufficio IT, e tiene conto delle persone, dei processi e della tecnologia; ciò permette al personale di comprendere quali rischi corre e di adottare i controlli di sicurezza come parte del lavoro quotidiano.

12. Approccio integrato

La Struttura generale ad alto Livello (High Level Structure) può essere definita come la struttura comune degli standard relativi ai sistemi di gestione, applicabile ai nuovi standard ISO e alle future revisioni di standard ISO esistenti. L'obiettivo è quello di uniformare la struttura e i contenuti chiave dei sistemi di gestione, per facilitarne l'integrazione e l'impiego da parte delle aziende e delle altre organizzazioni certificate.
Gli standard ISO oggetto della presente politica presentano una struttura suddivisa in 10 punti principali. Nell'ambito di ciascun punto, vi sono alcuni paragrafi e alcuni contenuti presenti obbligatoriamente in tutti gli standard. I singoli standard, inoltre, prevedono, ove necessario, requisiti specifici in relazione ai loro campi di applicazione.

L'approccio HLS punta all'uniformità della struttura degli standard ISO, da cui ne consegue una maggiore compatibilità tra le norme e la facilità nell'integrare i Sistemi di Gestione tra loro.
Nei paragrafi successivi si rimanda ai punti che prevedono una gestione similare nei diversi standard, ove è possibile avvalersi delle informazioni documentate già esistenti nell'Organizzazione, trasversali ai diversi sistemi di gestione, in particolare:

- Gestione del Rischio;
- Continuità Operativa;
- Audit interno;
- Riesame della direzione;
- Non conformità e Azioni correttive;
- Miglioramento continuo.

12.1. Gestione del rischio

La Gestione del Rischio (o Risk Management) è un insieme di attività, metodologie e risorse coordinate per guidare e tenere sotto controllo un'organizzazione con riferimento ai rischi. Un approccio globale al risk management consente all'Organizzazione di considerare il potenziale impatto delle diverse tipologie di rischio sui processi aziendali, sulle attività, sugli operatori, sui prodotti e sui servizi.
La gestione del rischio è strategica per la gestione operativa del SGI.
In un nuovo approccio alla gestione aziendale, la parte relativa alla gestione del rischio rappresenta un elemento fondamentale; questo sia riguardo alla sicurezza delle informazioni, sia in relazione al "miglioramento continuo".

La gestione del rischio si svolge a diversi livelli all'interno del SGI, compresi:

- la pianificazione della gestione dei rischi, per il conseguimento degli obiettivi;
- la valutazione del rischio in ambito di procedure di sicurezza del servizio ICT e di continuità operativa;
- la valutazione del rischio specifico associato al "cambiamento – rilascio - domanda" di prodotto, servizio o processo;
- come elemento strutturale del design di nuove soluzioni e per la transizione ai servizi modificati.

La valutazione del rischio viene rivista su base annuale o in seguito a un cambiamento significativo nel processo di business o nella fornitura del servizio.

12.2. La valutazione del rischio

Il processo di valutazione dei rischi è realizzato in modo che sia conforme con i requisiti e le raccomandazioni delle norme di riferimento. Ciò è documentato nel processo di valutazione dei rischi all'interno della documentazione di sistema.
Di conseguenza è richiesto che nel progetto di definizione di ogni singolo processo vengano identificati i seguenti aspetti:

- Asset;
- Conseguenze;
- Controlli;
- Minacce;
- Vulnerabilità;
- Impatto e probabilità prima del trattamento dei rischi;
- Trattamento del rischio (ad es. riduzione, eliminazione, trasferimento);
- Impatto e probabilità del rischio residuo dopo il trattamento.

Dall'analisi relativa viene generata una relazione di valutazione dei rischi, che è poi seguita da un piano di trattamento del rischio.

I dettagli del processo di gestione del rischio sono forniti all'interno del documento aziendale "Manuale del Sistema per la Gestione per la Sicurezza delle Informazioni" (MSGSI) e nel documento "SOA" (Statement Of Applicability/Dichiarazione di Applicabilità), ove sono identificati gli elementi di rischio, le vulnerabilità e i trattamenti.

12.3. Continuità Operativa

Per continuità operativa si intende la capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente. Tramite i modelli di gestione del rischio, le organizzazioni danno la percezione di tutela e creazione di valore per le parti interessate (azionisti, dipendenti, clienti, autorità di regolamentazione e pubblico in generale). Questo obiettivo è molto simile a ciò che è espresso quale fondamento logico per la continuità operativa. Quindi è chiaro che la gestione del rischio e la continuità operativa condividono una serie di caratteristiche.
Il risk management ha solitamente una più ampia portata rispetto alla continuità operativa, comportando in alcune grandi organizzazioni - specialmente nel settore finanziario - la necessità per la continuità operativa di adeguarsi al quadro complessivo dei rischi. A questo proposito è importante notare come la continuità

operativa si focalizzi - in particolare nella fase di Analisi - sull'identificazione delle vulnerabilità organizzative collegate al valore di base che supportano (Analisi delle Minacce) e sulla comprensione dell'impatto di una loro indisponibilità sull'Organizzazione (Business Impact Analysis).
La continuità operativa non è dunque solo identificazione, valutazione e segnalazione di ogni singolo rischio concepibile per un'organizzazione, i suoi mercati, i clienti e il contesto in cui opera e non è certamente mera assegnazione delle probabilità di manifestazione degli eventi. La gestione dei rischi identifica le minacce catastrofiche che sono al di fuori del controllo dell'organizzazione, mentre la gestione della continuità operativa si preoccupa di definire il modo per ridurre l'impatto di tali minacce, qualora si dovessero verificare.

La valutazione dei rischi che viene svolta all'interno di un programma di gestione della continuità operativa è di solito a livello operativo, in quanto riguarda l'interruzione delle attività. Tale valutazione dei rischi può integrare quella intrapresa come parte del programma di gestione dei rischi. L'implementazione di entrambe le discipline, continuità operativa e gestione dei rischi, fornisce a un'organizzazione l'opportunità di rafforzare la sua resilienza.

LAZIOcrea considera la continuità dei servizi erogati un bene fondamentale e prezioso, per cui pone la massima attenzione ed impegno nel garantirne la prosecuzione nel tempo e nello sviluppare la capacità di reagire a situazioni che possono causare l'interruzione o degrado delle proprie attività.
Al fine di garantire la continuità e la qualità dei propri servizi, coerentemente con le scelte strategiche dell'Organizzazione, risulta quindi fondamentale identificare in modo chiaro gli obiettivi per il SGCO che vengono applicati a livello aziendale.

12.4. Audit interno

L'Audit è un processo sistematico, indipendente e documentato per ottenere evidenze e valutarle con obiettività, al fine di stabilire in quale misura i criteri dell'audit sono stati soddisfatti.

Gli audit sono uno strumento principale della fase "check" del ciclo di Deming.
Gli audit interni, a volte denominati "audit di prima parte", sono effettuati per il riesame da parte dell'Alta Direzione, e possono costituire la base per una autodichiarazione di conformità da parte dell'Organizzazione.
La corretta impostazione di Audit Interni consente di comprendere se i diversi sistemi di gestione adottati dall'Organizzazione siano esattamente attuati o meno.

Il SGI prevede una serie di verifiche ispettive interne (o Audit Interni) volte a controllare la conformità delle attività dei processi e dei servizi alle rispettive norme, procedure e specifiche, verificando l'efficacia, l'attuazione e l'aggiornamento del sistema di gestione.
La verifica ispettiva interna è quindi uno degli strumenti utilizzati dall'Organizzazione per misurare lo stato del proprio SGSI e per sostenere il miglioramento continuo, promuovendo il ruolo della motivazione e della collaborazione, sempre nel rispetto dell'obiettività della verifica.
Il sistema delle verifiche ispettive interne, che è il complesso delle attività relative alla pianificazione, organizzazione e attuazione delle stesse e delle azioni collegate, è un elemento dinamico. La pianificazione delle verifiche ispettive interne tiene infatti conto, oltre che dei processi oggetto del sistema, dei risultati delle precedenti verifiche e delle criticità dei processi esaminati, ovvero le registrazioni delle valutazioni dei rischi e della dichiarazione di applicabilità, ovvero dell'Annex A della norma di riferimento.
L'Organizzazione predispone il piano delle verifiche ispettive interne tenendo conto dello stato e dell'importanza delle attività e delle aree da verificare, oltre che dei risultati di precedenti verifiche.
Vengono stabilite l'estensione di applicazione, la frequenza e le modalità delle verifiche. In particolare, su questo punto, le attività di controllo operative afferenti all'Annex A sono effettuate a campione e sulla base delle non conformità (NC) segnalate.
Il piano delle verifiche ispettive interne è impostato in modo da assicurare che ciascuna area funzionale sia esaminata almeno una volta all'anno. Il numero delle verifiche ispettive per ogni area dipende dalla sua importanza, criticità e influenza sull'efficacia del processo di erogazione del servizio nel suo complesso.
L'attività di auditing è effettuata da personale interno addestrato, o da consulenti esterni qualificati alla valutazione dei sistemi per la sicurezza delle informazioni. Gli auditor interni possono essere chiamati ad operare in tutti gli ambiti dell'azienda, ad esclusione del proprio settore di appartenenza e comunque non su attività per le quali sussistano dipendenze gerarchiche tra colui che ispeziona ed i responsabili di tali attività.
Il valutatore formalizza gli esiti della sessione in un rapporto di auditing. Le non conformità sono registrate su specifico sistema di registrazione e in primo luogo comunicate alla persona intervistata e al suo responsabile, per l'analisi delle cause e l'identificazione delle opportune azioni risolutive e correttive.
L'esito complessivo della verifica può essere oggetto di discussione in sede di riunione con il gruppo dei valutatori prima di essere oggetto di relazione verso l'Alta Direzione e i responsabili di area.
Le modalità operative di gestione delle verifiche ispettive interne sono riportate nel documento "Processo Gestione degli audit".

12.5. Riesame della Direzione

Il riesame della Direzione è un'analisi compiuta a intervalli regolari da parte del top management per verificare se gli obiettivi dei sistemi di gestione (qualità, sicurezza delle informazioni, continuità operativa, servizi IT) sono stati centrati e per valutare come correggere le proprie azioni nel caso in cui non lo siano stati.

È compito del top management effettuare un riesame del sistema di gestione con lo scopo di assicurarne la continua idoneità, adeguatezza ed efficacia. L'idoneità si riferisce all'allineamento coerente con gli obiettivi aziendali; l'adeguatezza e l'efficacia ad un buon inserimento del sistema all'interno dell'azienda, così come alla realizzazione dei processi e dei controlli definiti dal sistema stesso.
Complessivamente il riesame della Direzione è un processo realizzato a diversi livelli dell'Organizzazione; le sue attività vengono svolte in riunioni di divisione, che possono essere quotidiane, settimanali o mensili, così come in semplici incontri o tramite documenti che vengono condivisi.
Le responsabilità del riesame sono del top management, che si avvale di dati e informazioni che vengono da tutti i livelli dell'Organizzazione.
L'impegno dell'Alta Direzione verso lo sviluppo, l'attuazione e la gestione del SGSI è condotto attraverso attività atte ad impostare ed aggiornare il sistema in sede di riesame della Direzione. Alcune di queste sono:

- la promozione delle politiche e degli obiettivi per accrescere la consapevolezza, la motivazione ed il coinvolgimento del personale;
- l'identificazione dei processi di realizzazione che danno valore aggiunto all'Organizzazione;
- la pianificazione per il futuro dell'Organizzazione e per la gestione del cambiamento;
- la definizione e la divulgazione degli indirizzi mirati al conseguimento della soddisfazione delle parti interessate.

Durante l'attività di riesame del sistema, la Direzione:

- effettuata una valutazione delle policy di primo e secondo livello, per valutarne l'adeguatezza, ed eventualmente le aggiorna;
- esamina le esigenze di risorse e di comunicazioni necessarie ad assicurare che il sistema di gestione sia mantenuto e sviluppato, in linea con i cambiamenti della Organizzazione;
- identifica i processi operativi;
- identifica i processi di supporto, l'efficienza dei processi realizzativi, le esigenze delle parti interessate.

La Direzione analizza l'interazione dei processi, rivolgendo particolare attenzione a:

- assicurare che la sequenza e l'interazione dei processi siano concepite per il conseguimento dei risultati desiderati;
- assicurare che gli elementi in ingresso, le attività e gli elementi in uscita siano chiaramente definiti e controllati;
- monitorare gli elementi in ingresso e quelli in uscita per verificare che i singoli processi siano collegati fra loro ed operino in modo efficiente ed efficace;
- attivare un'analisi dei dati e dei KPI per facilitare il miglioramento continuativo in tutti i processi;
- individuare i responsabili di processo che abbiano la piena responsabilità ed autorità per raggiungere gli obiettivi stabiliti.

Il riesame di Direzione viene dettagliato nell'apposito processo.

12.6. Non conformità e Azioni correttive

La non conformità (NC) è il mancato soddisfacimento (totale o parziale) di un requisito da parte del Sistema di Gestione o una deviazione rispetto alle specifiche di riferimento.

I requisiti sono esigenze o aspettative che sono identificate, implicite o obbligatorie.
Le non conformità vengono solitamente rilevate dai valutatori nel corso delle visite ispettive.
L'Organizzazione reagisce sempre alle non conformità; ne valuta l'importanza e l'impatto, applica specifiche correzioni al problema (trattamento) e valuta specifiche azioni correttive, se necessario.
Ci sono diversi tipi di non conformità:

- il mancato rispetto di un requisito (completamente o parzialmente) della norma di riferimento da parte del sistema di gestione;
- la mancata attuazione o conformità ad un requisito, regola o controllo dichiarato all'interno del SGI;
- l'interruzione parziale o totale delle specifiche dei clienti, di legge o comunque concordate.

Estendendo l'accezione della definizione, possiamo classificare come NC anche:

- parametri e misurazioni fuori target, come sistemi di misura di gestione, processi, sicurezza o altro;
- obiettivi non raggiunti.

Le non conformità possono quindi anche essere, ad esempio:

- persone che non si comportano come previsto dalle procedure e dalle politiche;
- fornitori che non forniscono il prodotto o il servizio concordato;
- progetti che non producono i risultati attesi;
- controlli operativi fuori dal disegno / dalle impostazioni determinate.

Le non conformità possono essere riconosciute da:

- attività svolte in modo carente nel campo di applicazione del sistema di gestione;
- controlli inefficaci che non sono adeguatamente stabiliti;
- l'analisi degli incidenti di sicurezza dell'informazione che mostrano debolezze del sistema di gestione o dei controlli specifici;
- i reclami da parte dei clienti;
- gli avvisi degli utenti, personale, clienti e fornitori;
- monitoraggio e misurazione dei risultati che non soddisfano i criteri di accettazione;
- obiettivi non raggiunti.

Le correzioni (azioni risolutive o trattamento della NC) hanno lo scopo di affrontare immediatamente la non conformità e affrontare le sue conseguenze
Le azioni correttive mirano ad eliminare la causa di una non conformità e a prevenirne il ripetersi
Gli incidenti relativi alla sicurezza delle informazioni indicano l'esistenza di non conformità. Tuttavia, non si deve contare solo sugli incidenti per identificare le non conformità: audit, reclami dei clienti, comunicazione da parte di interni od esterni sono altre fonti importanti che aiutano a identificare una non conformità, o una potenziale non conformità.
La gestione delle non conformità viene dettagliato nell'apposito processo.

Il risultato complessivo del processo di gestione dovrebbe portare la non conformità ad uno stato gestito e controllato, anche in merito alle conseguenze associate.
Tuttavia, le correzioni da sole non necessariamente prevengono il ripetersi della non conformità

Le Azioni Correttive consistono in una serie di attività mirate a eliminare le cause di una non conformità rilevata o di altre situazioni indesiderabili rilevate. Le Azioni Correttive vengono attuate tutte le volte che si riscontrano NC (non conformità) di particolare rilevanza, o dopo avere constatato il verificarsi di NC simili, derivanti

da una singola od analoga causa. La profondità, l'estensione e la completezza delle azioni intraprese viene decisa di volta in volta, in funzione della loro importanza, criticità, costi e conseguenze.

12.7. Miglioramento

Per le norme contemplate nella presente politica (ISO 9001, ISO 27001, ISO 20000-1 e ISO 22301) il ciclo PDCA (Plan, Do, Check, Act) è il motore dello standard. L'infrastruttura dei sistemi di gestione in oggetto si basa quindi sul ciclo continuo di miglioramento applicato in modo ininterrotto sull'Organizzazione per verificare l'efficacia e l'efficienza nel conseguire i propri obiettivi.

La parte del miglioramento rappresenta la fase ACT della ruota di Deming.
Il miglioramento è un punto molto spesso sottovalutato o poco applicato, ma rappresenta l'essenza stessa di un sistema di gestione.

Un Sistema di Gestione (SG) è un elemento nato come qualcosa di "dinamico", che modifica le sue caratteristiche per meglio adattarsi ai cambiamenti o per migliorare le performance.
Non esiste un SG che si possa chiamare tale se i suoi connotati non si modificano nel tempo.
Le organizzazioni ed i loro contesti non sono mai statiche. Inoltre, i rischi per i sistemi informativi e le modalità con cui possono essere compromessi evolvono rapidamente. Infine, il SG, per quanto ben congegnato, non è perfetto, per cui c'è sempre un modo in cui può essere migliorato, anche se l'Organizzazione e il suo contesto non cambiano.

Nel valutare l'idoneità, l'adeguatezza e l'efficacia di un elemento del SGI, l'Organizzazione può prendere in considerazione se l'elemento supera notevolmente i requisiti di base del SGI. Se è così, allora può non esserci un'opportunità per migliorare l'elemento modificandolo, mentre è possibile la sostituzione o il ritiro dell'elemento stesso in modo che le risorse disponibili siano utilizzate in modo più efficiente.
Anche un approccio sistematico con il miglioramento continuo porta ad un SGI più efficace, che permette di migliorare la sicurezza delle informazioni dell'Organizzazione.
Il management dirige le attività operative al fine di evitare di essere troppo reattivi, per evitare che la maggior parte delle risorse vengano utilizzate per la ricerca di alcuni problemi e per affrontarli.

La base della funzionalità propria del SGI si concretizza attraverso il miglioramento continuo, in modo che l'Organizzazione possa avere un approccio più proattivo. Il top management può impostare obiettivi di miglioramento continuo, per esempio attraverso misure di efficacia, costi, o di maturità dei processi.
Di conseguenza, l'Organizzazione tratta il SGI come elemento vivo, concreto ed evoluto delle operazioni di business.
Affinché il SGI possa tenere il passo con i cambiamenti, deve essere regolarmente valutata la sua idoneità allo scopo, l'efficacia e l'allineamento agli obiettivi dell'Organizzazione. Nulla deve essere dato per scontato, e nulla è da considerarsi immodificabile semplicemente perché era abbastanza buono nel momento in cui è stato attuato.
La valutazione include un'analisi di:

- idoneità di elementi del SGI (compresi i controlli e processi di sicurezza delle informazioni), prendendo in considerazione se ci sono alternative possibili nella scelta, nei requisiti o nelle modalità di attuazione;
- l'adeguatezza del SGI e dei suoi elementi di pianificazione e progettazione, prendendo in considerazione se si sono evidenziati tutti gli obiettivi e le esigenze di sicurezza delle informazioni e se ci sono rischi che non sono stati identificati;
- l'efficacia del SGSI e dei suoi elementi, prendendo in considerazione se i risultati previsti sono raggiunti, se ci sono rischi sulla possibilità che non lo siano in futuro e se si intravedono possibili NC.