Sistemi di Gestione certificati

Politica della Qualità, dell'Ambiente e della Sicurezza delle Informazioni

Politica

Descrizione della policy aziendale in materia di Qualità
Descrizione della policy aziendale in materia di Ambiente
Descrizione della policy aziendale in materia di Sicurezza delle Informazioni

Redatta da	Verificata da	Approvata da	Revisione
Andrea Spila	*Renato Brunetti*	*DIR*	*04*
09.03.2022	09.03.2022	09.03.2022	09.03.2022

Sommario

Revisioni

Redatta da	Verificata da	Approvata da	Revisione
Andrea Spila	*Renato Brunetti*	*DIR*	*Prima edizione*
04/09/2018	19/09/2018	20/09/2018	0
18/01/2020	30/01/2020	20/02/2020	01
25/03/2020	26/03/2020	14/04/2020	02
11/11/2020	11/11/2020	11/11/2020	03
09/03/2022	09/03/2022	09/03/2022	04

1. Introduzione

1.1 Premesse e perimetro applicativo della norma

Lo scopo del presente documento (di seguito indicato come Politica per la qualità, l'ambiente e la Sicurezza delle Informazioni) è quello di descrivere i principi generali che UNIDATA ha fatto propri al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione Integrato rispettivamente ai sensi delle norme UNI EN ISO 9001:2015, UNI EN ISO 14001:2015 e ISO/IEC 27001:2017 con estensione ai requisiti delle norme (linee guida) ISO/IEC 27017:2021, e ISO/IEC 27018:2020.

Tali principi, come definito al Punto 4.4. del MQ, sono concretizzati in informazioni documentate proprie del Sistema (quali lo stesso MQ, le Procedure, le Istruzioni Operative, i Regolamenti e nella ulteriore documentazione in utilizzo aziendale - EL7.5.3A) ai fini del mantenimento di un Sistema di gestione della Qualità (SGQ) e della Sicurezza delle Informazioni (SGSI) così come genericamente definito al Punto 4.4 del relativo "Manuale", in relazione alle reali esigenze derivanti dalla tipologia di attività svolte da Unidata nello specifico ambito di applicazione delle suddette norme.

Le già menzionate informazioni documentate devono intendersi integrate dalle informazioni documentate proprie del Modello Organizzativo Privacy (MOP), applicato dall'Organizzazione in ottemperanza alle vigenti ed applicabili disposizioni normative, nazionali ed europee, in materia di trattamento dei dati personali quali:

- Regolamento UE 2016/679 – GDPR
- D.lgs. 196/03 così come modificato dal D.lgs. 101/2018
- Dai vigenti provvedimenti del Garante Privacy, tra i quali, a titolo esemplificativo:

  - Provvedimenti in materia di Amministratori di Sistema

  - Provvedimenti in materia di Trattamento dei dati biometrici

  - Provvedimenti in materia di Data Breach

  - ed ulteriori

e di cui il documento Data Protection Policy è espressione organica.

L'ambito di applicazione del Sistema di gestione della Qualità e per l'Ambiente (Punto 1.3 e 4.3 del MQ) e, conseguentemente, della presente Politica Unidata è stato definito come segue:

> *Erogazione Servizi di Accesso ad Internet, di telefonia e di Data Center (Cloud Computing, Hosting, Housing, Co-Location e Security Services) (IAF33). Progettazione, installazione, fornitura e manutenzione di Reti di telecomunicazioni e reti locali in fibra ottica e Internet of Things operanti mediante vari mezzi trasmissivi e diverse applicazioni (IAF28).*

L'ambito di applicazione del Sistema di Sicurezza delle Informazioni (Punto 1.3 e 4.3 del MQ) e, conseguentemente, della relativa Politica Unidata è stato definito come segue:

> *Gestione Infrastrutturale della sicurezza fisica e logica del proprio Data Center e delle relative Facility Management ed erogazione di servizi Cloud secondo i modelli IaaS e PaaS con l'applicazione delle linee guida ISO/IEC 27017 e ISO/IEC 27018 in accordo con la dichiarazione di applicabilità del 05 giugno 2020 (IAF 33)*

In accordo con la dichiarazione di applicabilità del 07.05.2021

Per l'attuazione delle attività di erogazione dei servizi già menzionati, l'Unidata si avvale, oltre che delle infrastrutture operative proprie della propria sede legale anche dell'infrastruttura, intesa in senso fisico e logico, denominata Internet Data Centre Unidata (di seguito IDC), sita anch'essa presso la sede legale della Unidata, in:

Roma, viale A. G. Eiffel, 100 – 00148 Roma c/o Commercity Mod. M26

Nella suddetta infrastruttura sono ospitati, in ambienti dotati di idonee misure di sicurezza infrastrutturali sia fisiche che logico-informatiche, sistemi ed apparecchiature di elaborazione/gestione dati (genericamente "apparati/server") come di seguito descritto:

- **server fisici e/o virtuali di proprietà della Unidata** e direttamente deputati all'esercizio dei sistemi informatici necessari a garantire la gestione della "mission aziendale" (**Sistemi aziendali "vitali" e/o "Critici")** cioè l'erogazione di servizi "informatici, di accesso ad Internet ed ulteriori di nuova generazione" all'utenza finale (Customer base);
- **server fisici e/o virtuali di proprietà della Unidata, affidati in gestione ad utenti finali/Clienti** (**Hosting**) per l'esercizio di servizi estranei alla competenza e responsabilità Unidata che rientrano nell'alveo di competenza e responsabilità della Unidata in relazione al loro corretto funzionamento in esercizio ed in relazione al rispetto degli obblighi di monitoraggio, sorveglianza e supporto nella repressione dei reati previsti dalla vigente normativa nazionale;
- **server fisici di proprietà dei Clienti ospitati** (**Housing**) presso detta infrastruttura per l'esercizio di servizi totalmente estranei alla competenza e responsabilità Unidata e totalmente e direttamente rientranti nell'alveo di competenza e responsabilità dell'utente/Cliente affidatario;
- **aree (perimetri fisici) in locazione esclusiva ad utente/Cliente** (**Co-location**) con o senza accesso alle facilities di cui al successivo punto

I suddetti locali afferenti all'infrastruttura IDC, oltre ad essere dotati di idonei servizi principali di c.d. "connettività" attraverso la presenza e disponibilità di "flussi" diversificati diretti alla gestione dell'interscambio dati su reti nazionali/internazionali con accesso alla Rete Internet, garantiscono anche i seguenti servizi strumentali (c.d. "facility"):

- sistema di controllo degli accessi
- sistema di videosorveglianza
- sistema di alimentazione elettrica diretta (sistema alimentazione primario) ed indiretta (sistemi di alimentazione di back up – UPS e gruppo elettrogeno di continuità)
- sistema di condizionamento ambientale ed allarmistica correlata
- sistema antincendio ed anti-allagamento
- sistemi di protezione logico informatica (firewalling – antivirus – etc.)
- sistemi di monitoraggio ed allarmistica sistemi
- sistema di assistenza sistemistica e/o di assistenza tecnica dedicata (ove contrattualizzati)

Attraverso detta infrastruttura e mediante ulteriori infrastrutture di servizio (fisiche e logiche) proprietarie o di terze parti, distribuite sul territorio, sono egualmente **assicurati servizi all'utenza finale** quali:

- Servizi di Accesso ad Internet wired/wireless, in fibra ottica(NGAN), rame e radio (hiperlan)

- Servizi di Telefonia vocale di rete fissa in tecnologia VoIP, di centralino remoto e virtuale, fax server

- Servizi di data centre (Housing, hosting, colocation, cloud, posta elettronica ed ulteriori)

Per una descrizione più esaustiva e dettagliata dell'infrastruttura nel suo complesso e delle misure di sicurezza nella stessa applicate, si rimanda ai seguenti documenti:

D7.1A Internet Data Centre
D7.1B – Infrastruttura di Rete

Quanto successivamente descritto nel presente documento e nella ulteriore documentazione di riferimento per il Sistema di Gestione della Qualità e per il Sistema di gestione della Sicurezza delle Informazioni, deve essere inteso, dunque, come applicato al suddetto perimetro fisico-logico nonché ai processi, risorse e/o rapporti lavorativi (Personale dipendente/Collaboratori/Terzi aventi causa) correlati e/o connessi alla debita gestione in esercizio della suddetta infrastruttura nell'ambito dei più ampi e generali scopi aziendali.

1.2 Obiettivi Generali del SGQ, del SGA e del SGSI

L'esistenza di un SGQ ha come obiettivo primario il raggiungimento e mantenimento di un livello qualitativo in continuo miglioramento nell'ambito del ciclo di erogazione del prodotto/servizio a favore dell'utenza finale.

Il SGSI ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.

In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- Integrità: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;

- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
- Autenticità: garantire la provenienza dell'informazione;
- Non ripudio: assicurare che l'informazione sia protetta da falsa negazione di ricezione, trasmissione, creazione, trasporto e consegna.

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità, Integrità, Autenticità e Non Ripudio, può comportare, nell'ambito di una qualsiasi attività aziendale, il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

La sicurezza delle informazioni è, quindi, un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia ed efficienza dei servizi erogati da Unidata. Di conseguenza, è essenziale per la società identificare le esigenze di sicurezza sia di natura esterna che derivanti dal cogente. Tale attività viene realizzata attingendo a diverse fonti:

- Analisi dei rischi: consente all'azienda di acquisire la consapevolezza e la visibilità sul livello di esposizione al rischio del proprio sistema informativo. Sulla base ditale livello sono individuate le misure di sicurezza idonee. La valutazione del rischio consiste nella sistematica considerazione dei seguenti elementi:
  - danno che può derivare dalla mancata applicazione di misure di sicurezza al sistema informativo, considerando le potenziali conseguenze derivanti dalla perdita di riservatezza, integrità, disponibilità, autenticità e non ripudio delle informazioni;
  - realistica probabilità di come sia possibile perpetrare un attacco alla luce delle minacce individuate.

I risultati della valutazione aiutano a determinare quali siano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee rispetto ai propri obiettivi, in base alla definizione del livello di rischio residuo che l'azienda decide di accettare, da implementare successivamente.

Per quanto sopra espresso, la presente policy, nel rispetto delle principali norme e degli standard in materia:

- sottolinea l'importanza di garantire la sicurezza delle informazioni e degli strumenti atti al trattamento delle stesse;
- è coerente con la volontà espressa dalla società di garantire la protezione del patrimonio informativo;
- ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Sicurezza delle Informazioni.

In particolare, la Politica della Qualità, dell'Ambiente e della Sicurezza delle Informazioni Unidata, intesa non soltanto come insieme di metodologie ma anche come comportamento manageriale, è diventata una leva strategica in tutte le attività orientate al cliente sia attraverso il migliore impiego delle risorse umane che finanziarie che tecnologiche. E' per questa ragione che UNIDATA si propone:

- l'obiettivo di garantire la completa soddisfazione delle aspettative del cliente attraverso l'erogazione di servizi di qualità frutto degli standard definiti nel proprio Sistema di Gestione per la Qualità.
- l'obiettivo di garantire la gestione in sicurezza delle informazioni essenziali per la continuità ed il miglioramento del business in linea ed in ottemperanza ai requisiti previsti dal proprio Sistema di gestione della Sicurezza delle Informazioni.

La Politica della Qualità, dell'Ambiente e della Sicurezza delle Informazioni della società UNIDATA si articola nei seguenti obiettivi generali:

- sviluppare e mantenere un Sistema di Gestione per la Qualità conforme agli standard UNI EN ISO 9001:2015 e UNI EN ISO 14001:2015 quale strumento per realizzare gli obiettivi, rispettare gli impegni assunti, promuovere il miglioramento continuo dei processi aziendali, garantire il rispetto dei requisiti cogenti per i prodotti ed i servizi correlati;

- sviluppare e mantenere un Sistema di Gestione della sicurezza delle Informazioni conforme allo standard ISO/IEC 27001:2017 e alle ISO/IEC 27017:2021 e ISO/IEC 27018:2020 quale strumento per controllare in modo sistematico e continuativo i processi che riguardano la sicurezza di tutto il patrimonio informativo aziendale, non solo dal punto di vista informatico (supporti elettronici o cartacei utilizzati per immagazzinare i documenti e i dati) ma soprattutto dal punto di vista gestionale ed organizzativo definendo ruoli, responsabilità e procedure formali per garantire l'adeguata operatività dell'azienda stessa.
- adottare un sistema integrato di gestione del rischio, al fine di garantire che per tutti i prodotti/servizi forniti il rischio residuo sia ridotto al minimo;
- diffondere la cultura dell'ambiente e dello sviluppo eco-sostenibile;
- massima attenzione ai rifiuti speciali prodotti, garantendo il massimo rispetto dell'ambiente e della normativa vigente;
- aumento della consapevolezza ambientale presso i principali stakeholder (soggetti interni o esterni all'impresa, con interessi ed esigenze diversi, in grado di influenzare le scelte e i comportamenti dell'impresa e di condizionarne il successo).
- impegnare tutte le energie e capacità a disposizione nell'ascoltare le indicazioni, suggerimenti, desideri del cliente, anche attraverso l'attività "on field";
- focalizzare ogni attività sui bisogni del cliente per soddisfarlo meglio e più velocemente in modo da affermare una posizione di leader nel mercato;
- consolidare il rapporto con i partner al fine di assicurare ai clienti prodotti di maggior valore, sicuri, affidabili, di alto livello tecnologico a prezzi ragionevoli;
- fornire prodotti e servizi aderenti a tutti i requisiti imposti dalle disposizioni legislative vigenti in materia;
- diffondere nell'organizzazione cultura e metodologie appropriate in modo che chiunque vi lavori sia costantemente in grado di erogare il miglior servizio atteso al cliente;
- assicurare un alto livello di soddisfazione di tutti i dipendenti attraverso la ricerca della massima lealtà e senso di responsabilità;
- incoraggiare il personale ed il management affinché possa realizzare le proprie attitudini, interessi e predisposizioni e sviluppi le proprie competenze tecniche ed organizzative;

La Direzione si impegna affinché gli obiettivi così definiti vengano compresi, accettati ed attuati a tutti i livelli dell'organizzazione attraverso:

- Impegno diretto, continuo e permanente nella gestione del Sistema di gestione Qualità, Sicurezza delle Informazioni e Ambiente;
- Coinvolgimento e partecipazione diretta, piena e consapevole del personale dell'azienda a tutti i livelli nell'attuazione del Sistema di gestione Integrato;
- Instaurazione di stretta collaborazione e trasparenza con i Fornitori per il miglioramento degli impatti ambientali dei prodotti/servizi acquistati;
- Impegno alla conformità legislativa in generale e in particolare in campo ambientale, alla prevenzione dell'inquinamento ed al miglioramento continuo

In particolare, per quanto concerne il SGA, Secondo l'Art. 5, comma c del D. Lgs. n. 152/2006, l'impatto ambientale è l'alterazione qualitativa e/o quantitativa, diretta ed indiretta, a breve e a lungo termine, permanente e temporanea, singola e cumulativa, positiva e negativa dell'ambiente, inteso come sistema di relazioni fra i fattori antropici, fisici, chimici, naturalistici, climatici, paesaggistici, architettonici, culturali ed economici, in conseguenza dell'attuazione sul territorio di piani o programmi o della realizzazione di progetti relativi a particolari impianti, opere o interventi pubblici o privati, nonché della messa in esercizio delle relative attività.

La Direzione consapevole dell'importanza che la tutela dell'ambiente ha per la propria immagine nonché delle proprie responsabilità nei confronti della salvaguardia del territorio circostante, ha deciso di dotarsi di un Sistema di Gestione Ambientale (SGA) tale da consentire la riduzione dei principali impatti ambientali e tenere sotto controllo gli aspetti correlati alla sua attività, assumendo così un ruolo attivo nei confronti dell'ambiente.

Unidata S.p.A., inoltre, ritiene di dover assumere nel perimetro di sua operatività la responsabilità in riferimento almeno ai seguenti *Obiettivi globali di Sviluppo Sostenibile ONU*[1]*:*

- la necessità di investimenti sostenibili nelle infrastrutture necessarie per la diffusione delle tecnologie di comunicazione;
- l'importanza della diffusione del modello di *smart city* per rendere le città inclusive, sicure, resilienti e sostenibili;
- promuovere l'efficienza nell'uso delle risorse e dell'energia;
- la necessità di agire rapidamente per combattere i cambiamenti climatici e i relativi impatti;
- la necessità di proteggere, ristabilire e promuovere l'uso sostenibile degli ecosistemi terrestri, la gestione sostenibile delle foreste, combattere la desertificazione, fermare e rovesciare la degradazione del territorio e arrestare la perdita della biodiversità.

Tale scelta presuppone come priorità aziendale la salvaguardia del territorio con l'impegno di utilizzare le risorse necessarie con la massima cura e con una gestione ambientale responsabile secondo un sistema volto al miglioramento continuo delle proprie prestazioni.

1.3 Obiettivi Operativi per l'anno di riferimento

L'Alta Direzione provvede poi su base annuale alla definizione e diffusione di un Piano contenente gli obiettivi per l'anno di riferimento che declinano in dettaglio gli obiettivi generali coinvolgendo i pertinenti livelli e le relative Funzioni aziendali nell'ambito dell'Organizzazione con il fine di aumentare/migliorare il livello di soddisfazione del Cliente e delle ulteriori Parti interessate.

Tale documento è indentificato come segue:

P6.2 Piano degli Obiettivi Operativi <anno di riferimento>

La presente Politica della Qualità, dell'Ambiente e della Sicurezza delle Informazioni è rivista ed aggiornata almeno con cadenza annuale nell'ambito della Revisione dell'Alta Direzione (Punto 9.3 della Norma) e/o all'esigenza.

La mancanza di adeguati livelli di qualità del prodotto/servizio, può comportare, nell'ambito di una qualsiasi attività aziendale, il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

[1] Assemblea Generale delle Nazioni Unite - New York 26-30/09/ 2015

La Qualità è, quindi, un requisito fondamentale per garantire l'affidabilità, l'efficacia e l'efficienza dei servizi erogati da Unidata. Di conseguenza, è essenziale per la società identificare le esigenze qualitative sia nei rapporti inter-aziendali (dipendenti/collaboratori) che nei rapporti con l'esterno (utenti/fornitori).
I risultati della valutazione aiutano a determinare quali siano le azioni necessarie per gestire i rischi individuati, le procedure e le misure più idonee rispetto ai propri obiettivi.

- **Principi ispiratori**: sono indicati nel Capitolo 2 della presente Politica intitolato "Policy". Rappresentano il sistema dei valori in cui l'azienda crede con riferimento alla gestione della qualità del proprio sistema produttivo/di erogazione. Si tratta delle idee di fondo che l'azienda ha maturato nei riguardi della qualità, ovvero che cosa sia giusto fare, o meno, per disporre di un sistema di gestione della qualità efficiente, efficace e adeguato alle proprie ed alle necessità del mercato. Il riferimento primario dei principi generali di sicurezza è lo standard UNI EN ISO 9001:2015 e UNI EN ISO 14001:2015.
- **Leggi e contratti:** nell'ambito del contesto normativo esistente, vengono fornite indicazioni su come affrontare le problematiche connesse al mantenimento di un livello qualitativamente alto nell'erogazione di servizi verso l'utenza, nell'esecuzione delle relative mansioni lavorative, nei rapporti con i fornitori, i collaboratori, i partner tecnico commerciali. Il rispetto della legislazione italiana relativa alla tutela e sicurezza nell'ambiente di lavoro, alla tutela dei Consumatori, alla correttezza nei rapporti professionali e commerciali, nonché il perseguimento costante di obiettivi di natura etica in tali ambiti serve, oltre che per limitare i rischi di un coinvolgimento dell'azienda, anche per garantire un livello adeguato di qualità del sistema produttivo aziendale.

La presente policy, nel rispetto delle principali norme, degli standard in materia e in combinazione con il documento specifico Data Protection Policy:

- sottolinea l'importanza di garantire la Qualità del prodotto/servizio e degli strumenti atti al raggiungimento e mantenimento della stessa;
- è coerente con la volontà espressa dalla società di garantire la soddisfazione dell'utente finale di detti prodotti/servizi;
- ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Qualità.

L'Alta Direzione si impegna inoltre a:

- **Divulgare e promuovere** la politica per la qualità;
- **Attuare** la politica per la qualità attraverso la definizione di obiettivi di miglioramento;
- **Riesaminare** la politica per la qualità in funzione dei risultati raggiunti e delle strategie aziendali.

E ad assicurare che:

- Le informazioni siano protette da accessi non autorizzati nel rispetto della riservatezza e siano disponibili solo agli utenti autorizzati;
- Le informazioni non vengano divulgate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;

- Vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- Il personale riceva addestramento sulla sicurezza delle informazioni;
- Tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed esaminati.

Attraverso l'attuazione di tale politica Unidata intende ottemperare all'impegno di conformità alla UNI CEI ISO/IEC 27001:2017, UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, ISO/IEC 27017:2021 e ISO/IEC 27018:2020 nonché di conseguire e mantenere tale certificazione. Per il conseguimento di tale obiettivo, la direzione si impegna a far si che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da collaboratori esterni e fornitori che siano in qualsiasi modo coinvolti con le informazioni aziendali.

1.2.2 Norme di standardizzazione comunitarie ed internazionali di riferimento

- UNI EN ISO 9001:2015 "Sistemi di Gestione per la qualità - Requisiti ".
- ISO 9000:2015 "Fondamenti e vocabolario dei sistemi di gestione per la qualità";
- ISO 3100:2010 "Risk Management"
- UNI EN ISO ISO/IEC 27001:2017 Sistemi di gestione della sicurezza delle informazioni – Requisiti.
- ISO/IEC 27017:2021 "Information technology- Security techniques-code of practice for information security controls based on ISO/IEC 27002 for cloud services ",
- ISO/IEC 27018:2020 "Information technology Security techniques Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"
- UNI EN ISO 14001:2015
- ISO/IEC 27002:2017 "Information technology Security techniques Code of practice for information security controls"
- ISO/IEC 27701:2019 "Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

1.2.3 Norme nazionali e di settore di riferimento

- D.lgs. 206/2005 Codice del Consumo
- D.lgs. 259/2003 Codice delle Comunicazioni Elettroniche
- D.Lgs.196/2003 Codice in materia di protezione dei dati personali come modificato dal D.lgs. 101/2018
- Regolamento EU 2016/679 General Data Protection Regulation (GDPR)
- D.lgs. 81/2008 e ss.mm. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro"

1.3. Informazioni Documentate (Documenti) del SGQ

L'elenco delle informazioni documentate del SGQ/SGA/SGSI Unidata, comprensivo della eventuale categoria di classifica è contenuto nel doc. EL7.5.3A. L'elenco è integrato dalle informazioni documentate relative al Modello Organizzativo Privacy (MOP) Unidata. Le registrazioni del SGQ/SGA/SGSI sono invece riportate nel documento EL7.5.3B.

1.4. Documenti del Sistema di Gestione per la Qualità

Nello specifico, possono ritenersi di diretta appartenenza al "Manuale del Sistema di gestione della Qualità, dell'Ambiente de e della Sicurezza delle Informazioni Unidata" i documenti risultanti dall'Elenco delle informazioni documentate - Documenti (EL7.5.3A) e le Registrazioni della Qualità riportate nell' Elenco delle informazioni documentate - Registrazioni (EL7.5.3B)

2 Policy

2.1 Principi generali della Qualità

I principi generali ai quali Unidata ispira la sua Politica di Qualità, nello specifico campo di applicazione del SGI Unidata di cui al Punto 1.1, sono articolati come segue:

- Assicurare che i requisiti dei Clienti siano ben definiti e parte fondamentale delle soluzioni proposte;
- Assicurare che le caratteristiche del prodotto o servizio offerto siano improntate al principio di massima informativa e trasparenza;
- Assicurare processi di delivery e maintenance chiari ed in costante miglioramento;
- Sforzarsi sempre di erogare ai Clienti un servizio in linea con le performance espresse nella Carta dei Servizi;
- Assicurare ad ogni livello aziendale una condotta rispettosa degli impegni presi nel Codice Etico Unidata;
- Tenere sempre in mente che l'unica ragione dell'esistenza di Unidata è nella qualità delle relazioni e nella qualità dei servizi offerti ai Clienti;
- Assicurare il rispetto della legislazione vigente;
- Assicurare la conformità del sistema di gestione;
- Assicurare l'adeguatezza della struttura e delle attrezzature.

In base a tali principi, nell'ambito del proprio SGQ, Unidata

Si impegna:

- verso i clienti, a fornire prodotti e servizi rispondenti ai requisiti cogenti e di qualità elevata, a dimostrare trasparenza ed affidabilità, ad assicurare la qualità del prodotto a prezzi competitivi, attraverso l'analisi ed il contenimento dei costi;
- verso i fornitori, a favorire una proficua "alleanza" in modo da poter essere parte attiva nella definizione delle prestazioni e delle caratteristiche del prodotto, ed a fornire il supporto necessario per la comprensione e definizione dei requisiti del Cliente e dei requisiti cogenti pertinenti il prodotto;
- verso i dipendenti a favorire lo spirito di iniziativa, incoraggiare la crescita professionale, assicurare rapporti professionali proficui e sereni, garantire un ambiente di lavoro sicuro nel quale tutti possano essere soddisfatti;
- verso la Proprietà a favorire la crescita dell'Azienda, assicurando adeguata redditività e stabilità finanziaria, elementi imprescindibili per l'affermazione della Politica per la qualità.

Si prefigge di:

- sviluppare e mantenere un Sistema di Gestione per la Qualità conforme allo standard UNI EN ISO 9001:2015, UNI EN ISO 14001:2015 alla norma ISO IEC 27001:2017 e ISO/IEC 27017:2021 e ISO/IEC 27018:2020 quale

strumento per realizzare gli obiettivi, rispettare gli impegni assunti, promuovere il miglioramento continuo dei processi aziendali, garantire il rispetto dei requisiti cogenti per i prodotti ed i servizi correlati;

- adottare un sistema integrato di gestione del rischio, al fine di garantire che per tutti i prodotti/servizi forniti il rischio residuo sia ridotto al minimo;
- impegnare tutte le energie e capacità a disposizione nell'ascoltare le indicazioni, suggerimenti, desideri del cliente, anche attraverso l'attività "on field";
- focalizzare ogni attività sui bisogni del cliente per soddisfarlo meglio e più velocemente in modo da affermare una posizione di leader nel mercato;
- consolidare il rapporto con i partner al fine di assicurare ai clienti prodotti di maggior valore, sicuri, affidabili, di alto livello tecnologico a prezzi ragionevoli;
- fornire prodotti e servizi aderenti a tutti i requisiti imposti dalle disposizioni legislative vigenti in materia;
- diffondere nell'organizzazione cultura e metodologie appropriate in modo che chiunque vi lavori sia costantemente in grado di erogare il miglior servizio atteso al cliente;
- assicurare un alto livello di soddisfazione di tutti i dipendenti attraverso la ricerca della massima lealtà e senso di responsabilità;
- incoraggiare il personale ed il management affinché possa realizzare le proprie attitudini, interessi e predisposizioni e sviluppi le proprie competenze tecniche ed organizzative;
- Comunicare ed aggiornare ogni anno gli orientamenti, gli impegni e gli obiettivi per la qualità;
- Convocare periodicamente specifiche riunioni, affinché ad ogni livello sia nota e condivisa la necessità di soddisfare i requisiti previsti dai contratti e capitolati e per effettuare gli aggiornamenti richiesti dall'evoluzione delle norme cogenti;
- Garantire che gli obiettivi della politica di qualità siano definiti e compatibili con il contesto e la direzione strategica della società e che comprendano la sicurezza delle informazioni;
- Garantire l'integrazione dei requisiti di sistema di gestione integrato nei processi di business aziendali.
- Comunicare la Politica aziendale con tutti i dipendenti.

Tende a:

- sviluppare tecniche di servizio pensate e realizzate per venire incontro alle esigenze del cliente, per anticiparne le aspettative, e fornire soluzioni che creino valore per il cliente;
- operare una selezione sistematica di nuovi prodotti di alto livello tecnologico;
- velocizzare la distribuzione di prodotti e servizi mediante l'adozione degli strumenti tecnici più innovativi ed affidabili, rendendo più efficiente l'organizzazione, utilizzando tutte le potenzialità necessarie.

L'operato di Unidata rispetta i seguenti principi:

- Collaborazione con gli Enti di certificazione;
- Collaborazione con i clienti.

2.2 Principi generali della Sicurezza delle Informazioni

I principi generali ai quali Unidata ispira la sua **Politica di Gestione della Sicurezza delle Informazioni**, nello specifico perimetro applicativo della norma di cui al Punto 1.1, sono articolati nelle seguenti tematiche:

- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici
- Norme comportamentali per la gestione sicura delle risorse aziendali

- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione della Business Continuity
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite da Unidata.

2.2.1 Identificazione, classificazione e gestione delle risorse

Obiettivo: *Tutto il personale di Unidata e, quando pertinente, i collaboratori, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività*

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo, un sistema di censimento di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad una Funzione aziendale responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro.
- Le modalità di gestione ed i sistemi di protezione per le informazioni e gli asset su cui risiedono devono essere coerenti con il livello di criticità identificato.

Punti della Norma:
7.2, Annesso A - ISO/IEC 27001:2017.

2.2.2 Gestione sicura degli accessi logici

Obiettivo: *garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.*

- L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (c.d. principio del "need-to-know"). La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.
- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinata al superamento di una procedura di identificazione ed autenticazione degli stessi.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
- E' necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

Punti della Norma:
11, Annesso A - ISO/IEC 27001:2017

2.2.3 Norme comportamentali per la gestione sicura delle risorse aziendali

Obiettivo: *garantire che i dipendenti e collaboratori di Unidata adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.*

- Gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
- I sistemi informatici aziendali devono essere impiegati da dipendenti e da collaboratori secondo procedure approvate.

Normativa nazionale:
Regolamento Generale per la Protezione dei dati (Regolamento UE 2016/679 - GDPR)
D.lgs. 101/2018 (Adeguamento nazionale al regolamento europeo in materia di privacy)
Punti della Norma:
8.2 e 11.1, Annesso A - ISO/IEC 27001:2017

2.2.4 Personale e sicurezza

Obiettivo: *garantire che il personale che opera per conto di Unidata (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.*

- Nelle fasi di selezione ed inserimento del personale in Unidata devono essere valutati i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte.
- Durante la permanenza in Unidata il personale deve ricevere un'adeguata e continuativa formazione inerente le tematiche di sicurezza dei dati.
- Le modalità di chiusura del rapporto di lavoro con Unidata dovranno essere coerenti con gli obiettivi di sicurezza aziendale.

Punti della Norma:
7.2, Annesso A -ISO/IEC 27001:2017

2.2.5 Gestione degli eventi anomali e degli incidenti

Obiettivo: *garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.*

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni.
- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.
- Deve esistere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

Punti della Norma:
16, Annesso A - ISO/IEC 27001:2017

2.2.6 Gestione della sicurezza fisica

Obiettivo: *prevenire l'accesso non autorizzato alle sedi ed ai singoli locali aziendali e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.*

- **Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite:**
  - l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate;
  - la definizione dei livelli adeguati di protezione;
  - la predisposizione di un ciclo periodico di verifiche e controlli.

- **Deve essere garantita la sicurezza delle apparecchiature tramite:**
  - la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
  - la messa a disposizione delle risorse necessarie al loro funzionamento;
  - la predisposizione di un adeguato livello di manutenzione;
  - la predisposizione di un ciclo periodico di verifiche e controlli.

Punti della Norma:
11.1, Annesso A -ISO/IEC 27001:2017

2.2.7 Gestione della sicurezza delle informazioni per i servizi cloud

Cliente servizio Cloud	Fornitore di servizi di cloud (Unidata)
Il cliente del servizio cloud è correttamente informato per tutto ciò che concerne i seguenti aspetti: - Le informazioni memorizzate in ambiente di cloud computing possono essere oggetto di accesso e di gestione da parte di Unidata; - Le risorse sono mantenute in ambiente cloud computing; - Gli amministratori di servizi cloud hanno un accesso privilegiato.	Unidata fornisce garanzie in merito ai seguenti aspetti: - Requisiti di sicurezza delle informazioni di base applicabili alla progettazione e all'implementazione del servizio cloud - Garanzia in merito alle procedure di controllo di accesso - Pronta comunicazioni durante la gestione dei cambiamenti - La garanzia della protezione dei dati - La gestione del ciclo di vita degli *account* dei clienti - La comunicazione di violazioni e linee guida per la condivisione delle informazioni a supporto di indagini e analisi forensi

2.2.8 Aspetti contrattuali connessi alla sicurezza delle informazioni

Obiettivo: *assicurare la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che Unidata deve instaurare con le terze parti stesse.*

- Gli accordi con le terze parti e con gli outsourcer che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.
- Gli accordi con terze parti e con gli outsourcer, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali ("normativa privacy").

Normativa nazionale:
Regolamento Generale per la Protezione dei dati (Regolamento UE 2016/679 - GDPR)
D.lgs. 101/2018 (Adeguamento nazionale al regolamento europeo in materia di privacy)
Punti della Norma:

6.1, 15 e 18.1, Annesso A -ISO/IEC 27001:2017

2.2.9 Gestione della Business Continuity

Obiettivo: *garantire la continuità dell'attività di Unidata e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale.*

- Devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business.
- Deve essere predisposto un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sulla missione aziendale.
- Devono essere preparate, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità.
- Devono essere periodicamente effettuati i test per tutti i componenti del piano di continuità.
- Deve essere assicurato il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

Punti della Norma:

17.1, Annesso A - ISO/IEC 27001:2017

2.2.10 Monitoraggio, tracciamento e verifiche tecniche

Obiettivo: *garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.*

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.
- A fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.
- Devono essere pianificate attività periodiche di audit del sistema di gestione della sicurezza delle informazioni.

Punti della Norma:

16.1, Annesso A - ISO/IEC 27001:2017

2.2.11 Ciclo di vita dei sistemi e dei servizi

Obiettivo: *assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.*

- Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:
  - inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi;
  - adozione di best practice per lo sviluppo e la manutenzione del software;
  - gestione controllata della documentazione;
  - separazione degli ambienti di sviluppo e test con impiego di procedure formali di accettazione nel passaggio fra ambienti.
- Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:
  - capacity management dell'infrastruttura tecnologica;
  - securizzazione dei sistemi e dei dati (configuration management, hardening, installazione di sistemi anti-malware, crittografia);
  - utilizzo di procedure di change management;
  - adozione di procedure di backup e restore;

- adozione di procedure di dismissione controllata dei sistemi (per esempio cancellazione sicura dei dischi);
- network security: segregazione delle reti, monitoraggio dei gateway (firewall).

- Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:
  - monitoraggio dei sistemi e servizi;
  - gestione utenze;
  - performance monitoring.

Punti della Norma:

12, Annesso A - ISO/IEC 27001:2017

2.2.12 Rispetto della Normativa

Obiettivo: *garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.*

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi.
- I responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati.
- Il mancato rispetto di quanto indicato in questo documento, e in tutti gli altri che da esso discendono, sarà gestito in ottemperanza a quanto previsto nel CCNL oppure, nel caso di inadempienze di terze parti, secondo i rapporti contrattuali in essere.

Punti della Norma:

15, Annesso A -ISO/IEC 27001:2017

2.2.13 Sicurezza dei dati dei clienti gestiti tramite i servizi IaaS, PaaS e SaaS venduti

UNIDATA ha sempre fatto della sicurezza delle informazioni e della salvaguardia delle stesse un fiore all'occhiello dei propri sistemi.
Oltre a tutti i sistemi di protezione dei dati da attacchi esterni, backup degli stessi e sistemi di disaster recovery all'avanguardia, Unidata ha deciso di adottare, al fine di tutelare le informazioni di accesso dei propri utenti, un sistema organico di misure di sicurezza, di procedure gestionali nonché un impianto documentale idonei e conformi ai requisiti nazionali ed europei in materia di trattamento dei dati personali (Data Protection Policy - Misure di sicurezza generali e particolari) ed ai requisiti previsti dalle norme a certificazione volontaria (ISO/IEC 27001; ISO/IEC 27017 e ISO/IEC27018) quale integrazione sinergica, calibrata sulla natura dei servizi erogati ai Clienti, ai sistemi gestionali già in essere.

3 Definizione dei ruoli e delle responsabilità

3.0 Responsabilità del sistema di gestione ambientale

La Direzione si assume la responsabilità di stabilire e diffondere la Politica dell'Ambiente all'interno e all'esterno dell'Azienda assicurandosi che essa sia:

- *documentata, compresa, sostenuta, attuata e diffusa a tutto il personale;*

- *disponibile a chiunque ne faccia richiesta.*

È responsabilità della Direzione intervenire tempestivamente per i problemi di gestione ambientale che non potranno essere risolti autonomamente dalle strutture organizzative preposte.

UNIDATA SPA effettua un'analisi costante delle interazioni delle proprie attività con il contesto e, al fine di mantenere il Sistema di Gestione Ambientale attivo e dinamico predispone annualmente un sistema di obiettivi e traguardi misurabili tramite l'utilizzo di indicatori e un programma di monitoraggio degli stessi che possa garantire l'efficacia e l'efficienza del sistema stesso. L'analisi dei dati fornisce informazioni utili per la successiva definizione di interventi e di azioni mirate alla prevenzione o mitigazione degli aspetti più significativi emersi.

La Direzione è coinvolta in prima persona nel rispetto e nell'attuazione di questi principi assicurando e verificando periodicamente che la presente Politica sia documentata, implementata, mantenuta attiva, diffusa a tutto il personale e resa disponibile al pubblico.

Il processo sotteso a detto coinvolgimento, in conformità allo standard in uso nei sistemi gestionali aziendali, si articola nelle seguenti macro-fasi che si applicano con sequenza ciclica secondo una logica c.d. PDCA[2]

- analisi dei processi e individuazione degli impatti ambientali collegati e loro misura attraverso specifici indicatori;
- attribuzione di ruoli e responsabilità e definizione di obiettivi e traguardi e allocazione di un budget adeguato;
- pianificazione, valorizzazione ed implementazione delle azioni di miglioramento;
- verifica periodica dell'efficacia delle azioni messe in campo e reporting del progresso verso il raggiungimento di obiettivi e traguardi;
- riesame del processo ed eventuale rimodulazione del piano d'azione.

3.1 Struttura responsabile della gestione della sicurezza delle informazioni

La struttura responsabile del sistema di gestione della sicurezza delle informazioni dovrà farsi promotrice, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni;
- risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione perla sicurezza delle informazioni.

Normativa nazionale:

DOC RFC_2350 V.1.6 25/02/2015

Art. 16bis c4 D.Lgs. n. 70/2012

DPCM 24/01/2013

[2] La costruzione di un sistema di gestione, in generale, passa attraverso quattro fasi, cioè:
Plan = pianificazione (che comprende la definizione della politica e del programma);
Do = attuazione (che comprende la definizione delle procedure di sistema);
Check = verifica (che comprende il monitoraggio, le registrazioni e le verifiche);
Act = azione (le azioni con cui intervenire per apportare modifiche e migliori e si decidono con il riesame del sistema da parte della Direzione).

DPCM 158/2013

Provvedimento su gestione eventi data Breach Garante Privacy

Punti della Norma:

6.1e 18, Annesso A -ISO/IEC 27001:2017

3.2 Management e Funzione SEC

Il Management (Direzione) è la funzione aziendale apicale a cui competono, con il supporto della funzione direzionale principale SEC (Security) e della struttura responsabile del sistema di gestione della sicurezza delle informazioni (Resp. SGSI), le decisioni di massimo livello riguardo alle tematiche di sicurezza.

In particolare, ha la responsabilità di supportare e garantire, mediante le funzioni aziendali subordinate, l'applicazione delle politiche generali del Sistema di Gestione della Sicurezza delle Informazioni, di definire le politiche idonee di gestione del rischio e di supportare costantemente il processo di sensibilizzazione sulle tematiche di sicurezza.

Punti della Norma:

Cap. 5 e 7 ISO/IEC 27001:2017

5.1, Annesso A -ISO/IEC 27001:2017

4 Conclusioni

La presente Politica per il sistema di gestione della Qualità, per l'ambiente e per la sicurezza delle informazioni, costituisce in materia, l'indirizzo al quale tutto il personale è tenuto a conformarsi nello svolgimento delle proprie mansioni e il quadro di riferimento per la pianificazione e gestione delle proprie attività e il riesame degli obiettivi e traguardi stabiliti.

L'Organizzazione effettua verifiche interne periodiche dirette a valutare l'efficacia e l'adeguatezza del proprio SGI. I risultati di queste verifiche vengono riesaminati dalla Direzione per individuare e programmare azioni e interventi che consentano un miglioramento continuo delle prestazioni.

Il presente documento è revisionato annualmente in occasione della riunione per la redazione del Riesame della Direzione.

Roma, 09/03/2022

La Direzione Aziendale