TRENTINO DIGITALE S.P.A.

Politica Generale di Sicurezza

1 PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
	01.0 Obsoleta	Prima emissione
	01.1 Obsoleta	Sostituzione del riferimento SIC-POL-06 (soppressa) con SIC-POL-10.
	02.0 Obsoleta	Modifiche a seguito dell'aggiornamento della norma ISO27001
	03.0 Obsoleta	Adeguamento a seguito del nuovo asset aziendale
19/09/2019	04.0 Obsoleta	Aggiornamento template documento.
16/10/2020	04.1 In vigore	Adeguamento a seguito dell'adozione delle estensioni di controlli previste dalla ISO/IEC 27017:2015 e ISO/IEC 27018:2014

INDICE

1 Introduzione

1.1 Premessa

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni che Trentino Digitale ha fatto propri al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Tali principi sono concretizzati nelle Policy per la sicurezza delle informazioni (nonché sintetizzati all'interno del *"Manuale della Qualità"*), la quale rispecchia le reali esigenze derivanti dalla tipologia di attività svolte da Trentino Digitale.

La sicurezza delle informazioni 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;

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità e Integrità, 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 Trentino Digitale. 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 di tale 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.

- Principi ispiratori: sono indicati nel Capitolo 2 intitolato "Policy". Rappresentano il sistema dei valori in cui l'azienda crede con riferimento alla gestione della sicurezza del proprio sistema informativo. Si tratta delle idee di fondo che l'azienda ha maturato nei riguardi della sicurezza delle informazioni, ovvero che cosa sia giusto fare, o meno, per disporre di un sistema di gestione della sicurezza efficiente, efficace e adeguato alle proprie necessità. Il riferimento primario dei principi generali di sicurezza è lo standard UNI CEI ISO/IEC 27002:2014.
- Leggi e contratti: nell'ambito del contesto normativo esistente, vengono fornite indicazioni su come affrontare le problematiche della sicurezza e su come gestire l'utilizzo dei sistemi informativi. Il rispetto della legislazione italiana relativa alla sicurezza serve, oltre che per limitare i rischi di un coinvolgimento dell'azienda, anche per garantire un livello minimo di sicurezza del sistema informativo da proteggere.

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.

1.2 Perimetro Organizzativo

La presente policy si applica a tutto il personale dipendente di Trentino Digitale e a tutti i soggetti che collaborano con Trentino Digitale.

La policy si applica inoltre a tutti i processi più in generale e a tutte le risorse coinvolte nella gestione delle informazioni trattate dalla società.

1.3 Termini e definizioni

Asset o Bene – Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (es. beni fisici, software, informazioni e dati, …).

Autenticità – Proprietà per la quale è garantito che l'identità di un soggetto o di una risorsa è quella dichiarata; l'autenticità si applica ad entità quali utenti, processi, sistemi ed informazioni (ISO/IEC 13335-1:2004).

Autorizzato al trattamento – la persona fisica che è autorizzato a trattare dati personali per conto del titolare del trattamento ovvero per conto del responsabile o del sub-responsabile del trattamento.

Disponibilità – Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata (ISO/IEC 13335-1:2004).

Hardening – *Insieme* di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.

Integrità – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata (ISO/IEC 13335-1:2004).

Interessato – soggetto i cui dati personali sono trattati.

Non ripudio – Capacità di dimostrare che un'azione o un evento hanno avuto luogo, in modo che questo evento od azione non possano essere ripudiati successivamente (ISO/IEC 13335-1:2004).

Responsabile del trattamento – la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Riservatezza – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO/IEC 13335-1:2004).

Sub-responsabile del trattamento – la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di un Responsabile del Trattamento;

Titolare del trattamento – la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

1.4 Riferimenti

Norme di legge	*Regolamento (UE) 2016/679 "Regolamento generale sulla protezione dei dati"* *D.lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss. mm. ii.* D.lgs. 196 del 30/06/2003 "Codice in materia di protezione dei dati personali"
Standard di Riferimento	UNI CEI ISO/IEC 27001:2014 – "Tecnologie Informatiche – Tecniche per la Sicurezza – SGSI - Requisiti"

	UNI CEI ISO/IEC 27002:2014 - "Tecnologie Informatiche – Tecniche per la Sicurezza – Raccolta di prassi sui controlli per la sicurezza delle informazioni" ISO/IEC 27017:2015 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services" ISO/IEC 27018:2014 " Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" ISO/IEC 13335-1:2004 - "Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management"
A documenti del Sistema Sicurezza	SIC-LG-04 "Regolamento sul corretto utilizzo delle risorse aziendali – dipendenti" SIC-LG-05 "Regolamento sul corretto utilizzo delle risorse aziendali – terze parti" SIC-LG-03 "Disciplinare di gestione impianto videosorveglianza" SIC-POL-11 "Sicurezza fisica e ambientale" SIC-POL-02 "Personale e sicurezza" SIC-POL-03 "Definizione ed assegnazione dei profili di accesso ai trattamenti" SIC-POL-04 "Aspetti contrattuali connessi con la sicurezza delle informazioni" SIC-POL-05 "Identificazione, classificazione e gestione degli asset" SIC-POL-07 "Gestione degli incidenti di sicurezza" SIC-POL-08 "Sicurezza nella progettazione e sviluppo di soluzioni informatiche" SIC-POL-10 "Sicurezza nell'esercizio e gestione di soluzioni

	informatiche” SIC-POL-12 “Gestione Continuità Operativa e Disaster Recovery” SIC-POL-13 “Gestione Sicurezza nel Cloud”
A documenti del Sistema di Gestione per la Qualità	SGQ-MQ-01 “Manuale della Qualità”

2 Policy

2.1 Principi Generali

I principi generali cui Trentino Digitale si ispira nella gestione della sicurezza delle informazioni 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
- Protezione dei dati personali
- Puntuale individuazione delle responsabilità nell’ambito del trattamento di dati personali
- Gestione della sicurezza nel Cloud
- Rispetto della normativa

Di seguito, si riporta, per ciascuna tematica, l’obiettivo e le linee guida definite da Trentino Digitale.

2.2 Identificazione, classificazione e gestione delle risorse

Obiettivo: garantire la piena conoscenza delle informazioni gestite in Trentino Digitale e la valutazione della loro criticità, al fine di agevolare l’implementazione degli adeguati livelli di protezione.

- 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 un 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.

I principi generali espressi nel presente paragrafo fanno riferimento ai punti 6.2 e 8, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-05 *"Identificazione, classificazione e gestione degli asset".*

2.3 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 subordinato 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.
- È 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare ai punti 9 e 13.1.3, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-10 "*Sicurezza nell'esercizio e gestione di soluzioni informatiche"* e all'interno del documento SIC-POL-03 *"Definizione ed assegnazione dei profili di accesso ai trattamenti"*.

2.4 Norme comportamentali per la gestione sicura delle risorse aziendali

Obiettivo: garantire che i dipendenti e collaboratori di Trentino Digitale 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 dai collaboratori secondo procedure approvate.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare alle principali richieste provenienti dal Codice in materia di tutela dei dati personali (D.lgs. 196/2003) e dall'Allegato A dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-LG-04 *"Regolamento sul corretto utilizzo delle risorse aziendali – dipendenti"* e all'interno del documento SIC-LG-05 *"Regolamento sul corretto utilizzo delle risorse aziendali – terze parti"*.

2.5 Personale e sicurezza

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

- Nelle fasi di selezione ed inserimento del personale in Trentino Digitale 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 Trentino Digitale il personale deve ricevere un'adeguata e continuativa formazione inerente alle tematiche di sicurezza dei dati.
- Le modalità di chiusura del rapporto di lavoro con Trentino Digitale dovranno essere coerenti con gli obiettivi di sicurezza aziendale.

I principi generali espressi nel presente paragrafo fanno riferimento ai punti 6.1.1, 7, 8.1.4 e 9.2.6, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-02 *"Personale e sicurezza"*.

2.6 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 16, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-07 *"Gestione degli incidenti di sicurezza"*.

2.7 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.
- 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 11, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-11 *"Sicurezza fisica e ambientale"* e all'interno del documento SIC-LG-03 *"Disciplinare di gestione impianto videosorveglianza"*.

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 Trentino Digitale 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").

I principi generali espressi nel presente paragrafo fanno riferimento in particolare alle principali richieste provenienti dal Codice in materia di tutela dei dati personali (D.lgs. 196/2003) e al punto 15, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-04 *"Aspetti contrattuali connessi con la sicurezza delle informazioni"*.

2.9 Gestione della Business Continuity

Obiettivo: garantire la continuità dell'attività di Trentino Digitale 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 17, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-12 *"Gestione Continuità Operativa e Disaster Recovery"*.

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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare ai punti 12.4, 18.2 e 12.7, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014.

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, anche a protezione di eventuali dati personali trattati, 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare ai punti 10, 12, 13 e 14, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014 e sono riportati con maggiore dettaglio all'interno del documento SIC-POL-08 *"Sicurezza nella progettazione e sviluppo di soluzioni informatiche"* e SIC-POL-10 *"Sicurezza nell'esercizio e gestione di soluzioni informatiche"*.

2.12 Protezione dei dati personali

Obiettivo: garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla protezione, alla gestione e alla conservazione dei dati personali, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

Per Sicurezza dei Dati Personali si intende il rispetto "*…della dignità umana, dei diritti e delle libertà fondamentali della persona*", attraverso il soddisfacimento dei seguenti requisiti:

- **Riservatezza del dato**: al fine di impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento dei dati personali.
- **Integrità del dato**: al fine di impedire la modifica non autorizzata dei dati personali e delle attrezzature impiegate per il trattamento dei dati Personali;
- **Disponibilità del dato**: i dati personali devono essere accessibili dagli interessati quando richiesto, in linea con i livelli di sicurezza definiti e nel rispetto dei diritti dello stesso.

Questi requisiti vengono perseguiti in ogni fase del ciclo di vita del trattamento del Dato Personale. I dati personali devono essere "*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*".

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 5, Allegato A, della norma UNI CEI ISO/IEC 27001:2014, esteso ai controlli previsti nella norma ISO/IEC 27018:2014 per i trattamenti svolti in ambiente cloud.

2.13 Puntuale individuazione delle responsabilità nell'ambito del trattamento di dati personali

Obiettivo: garantire che gli accordi contrattuali identifichino chiaramente le diverse responsabilità, legate alle operazioni di trattamento dei dati personali, in capo a Trentino Digitale, eventuali suoi subappaltatori e il cliente anche dipendentemente dalla tipologia del servizio.

I ruoli che devono essere previsti, in particolare nei contratti di erogazione del servizio e nei contratti con i subappaltatori, sono quelli previsti dalla normativa di riferimento sulla privacy ovvero:

- **Titolare del trattamento**
- **Responsabile del trattamento**
- **Sub-responsabile del trattamento**
- **Autorizzato al trattamento**
- **Interessato**

Questi requisiti vengono soddisfatti tramite idonei negozi giuridici concordati tra le parti prima che inizi il trattamento dei dati personali.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 5, Allegato A, della norma UNI CEI ISO/IEC 27001:2014, esteso ai controlli previsti nella norma ISO/IEC 27018:2014 per i trattamenti svolti in ambiente cloud.

2.14 Gestione della sicurezza nel cloud

Obiettivo: garantire la corretta gestione delle informazioni memorizzate su cloud, sia che l'azienda utilizzi i servizi di terzi o fornisca servizi basati sul cloud ai suoi clienti, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.

- Quando l'organizzazione usufruisce di servizi Cloud erogati da terzi: 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.
- 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 5, Allegato A, della norma UNI CEI ISO/IEC 27001:2014, esteso ai controlli previsti nella norma ISO/IEC 2717:2015, e

sono riportati con maggiore dettaglio all'interno del documento SIC-POL-13 *"Gestione sicurezza Sicurezza nel Cloud"*.

2.15 Rispetto della normativa

Obiettivo: garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla 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.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al punto 18 e 12.7, Allegato A, dello standard UNI CEI ISO/IEC 27001:2014.

3 Definizione dei Ruoli e delle Responsabilità

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 per la sicurezza delle informazioni.

3.2 Comitato privacy e sicurezza

Il Comitato Privacy e Sicurezza è l'organismo a cui competono, con il supporto della struttura responsabile del sistema di gestione della sicurezza delle informazioni, le decisioni di massimo livello riguardo alle tematiche di sicurezza.

In particolare, ha la responsabilità di supportare e garantire 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.

Il Comitato dovrà riunirsi con frequenza annuale, o con frequenza maggiore qualora intervengano modifiche significative dell'organizzazione o al contesto di riferimento.

3.3 Struttura Responsabile della Gestione Privacy

La struttura responsabile della gestione della privacy funge da punto di contatto con i clienti, interni ed esterni, oltre che con i fornitori per tutte le tematiche connesse al trattamento di dati personali.