



Let the future in

**POLITICA PER LA QUALITÀ  
E  
LA SICUREZZA DELLE INFORMAZIONI**

**MOD-520  
REV. 0.2 DEL 08/01/2024**

## 1. POLITICA PER LA QUALITA'

La politica per la qualità della società DIGIT CONSULTING S.r.l. vuole essere, prima che una metodologia di lavoro, una forma di pensiero. L'attenzione alla qualità è mirata, oltre che alla soddisfazione del cliente, al rispetto profondo per la persona, per la professionalità, nella convinzione che il lavoro, creativo e consapevole, è una dimensione qualificante dell'esperienza umana.

La DIGIT CONSULTING S.r.l. ha stabilito, nelle direttive aziendali, di considerare la Qualità come elemento determinante per i prodotti realizzati e servizi offerti. Questa politica della Qualità viene perseguita e rimane come punto di riferimento costante per tutte le sue azioni. Tra i possibili modi per il raggiungimento ed il mantenimento di un elevato livello di Qualità, la società ha stabilito di dotare l'azienda di un SGQ conforme alla norma UNI EN ISO 9001:2015 e idoneo al raggiungimento degli obiettivi.

In questo contesto:

- ✓ Il SGQ non deve essere una sovrastruttura che ingabbia e costringe, ma il quadro di riferimento formale di uno stile di lavoro che ha come obiettivi l'attenzione al particolare e la soddisfazione del cliente;
- ✓ Le metodologie di lavoro adottate devono mirare alla soddisfazione del cliente attraverso l'individuazione chiara dei requisiti. La logica "pensare", "fare", "verificare" e "migliorare" deve essere applicata a tutti i processi; sia quelli attraverso i quali si realizzano i prodotti per i clienti, sia quelli concernenti l'organizzazione stessa. A ciascuno è richiesto l'impegno a rendere sempre più efficace il sistema, nella convinzione che un SGQ che "nasce dal basso" renda partecipe ciascuno della sua applicazione;
- ✓ È molto importante che ciascuno sia consapevole della necessità di applicare una logica di miglioramento continuo, a tutti i livelli. A questo proposito, più che una comunicazione di tipo gerarchico, per far crescere tale consapevolezza, appaiono utili la discussione e la dialettica all'interno dei gruppi di lavoro;
- ✓ Mantenere alta l'attenzione ai principi di sostenibilità ambientale in quanto oggi la qualità non si deve limitare solo ai processi e ai prodotti/servizi, ma si estende anche all'ambiente di lavoro interno, alla formazione e alla sicurezza del personale, nonché al rispetto dell'ambiente esterno;
- ✓ Le attività del riesame del SGQ devono essere momenti costruttivi, per individuare le possibilità di miglioramento e verificare l'effettiva idoneità del sistema alle esigenze dell'organizzazione. Gli obiettivi sono individuati in sede di riesame del SGQ e comunicati all'organizzazione;
- ✓ Il quadro strategico definito mira innanzitutto ad ottenere la conformità dei prodotti realizzati, migliorandone la tecnologia, diminuendo le difettosità e aumentando la capacità dell'assistenza post-vendita di fornire risultati migliori.

## 2. POLITICA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

### 2.1. Contenuto

Le informazioni devono essere gestite in modo sicuro, accurato e affidabile e devono essere prontamente disponibili per gli usi consentiti. È utile sottolineare che per “utilizzo dell’informazione” si intende qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale. La norma ISO/IEC 27001:2022 prevede che il responsabile della sicurezza svolga periodicamente una “valutazione dei rischi” tenendo chiaramente in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi nel periodo e dei cambiamenti strategici di business e tecnologici accaduti; tale analisi dei rischi ha lo scopo di valutare il rischio di ogni asset (o beni con valore utilizzati nella tecnologia dell’informazione o comunicazione) da proteggere rispetto alle minacce individuate. La direzione condivide con il responsabile della sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella metodologia della redazione inoltre la direzione partecipa alla definizione dei parametri ed alla scala dei valori da impiegare, considerando al termine della valutazione i risultati ottenuti accettando la “soglia di rischio accettabile”, il “trattamento di mitigazione dei rischi” oltre tale soglia, ed il rischio residuo a seguito del trattamento. Tale analisi sarà ponderata anche rispetto al valore del business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere e da classificare secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti. Detta analisi dovrà inoltre essere elaborata ogni qualvolta si verificano cambiamenti tali da incidere sul profilo del rischio complessivo del sistema.

#### 2.1.1 Obiettivi

L’obiettivo del sistema di gestione della sicurezza delle informazioni in DIGIT CONSULTING è quello di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell’ambito del campo di applicazione definito (Progettazione, sviluppo, installazione e manutenzione di siti web ed applicativi per servizi su dispositivi automatici non presidiati. Installazione, assistenza e manutenzione hw e sw su postazioni di lavoro) tramite l’identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il sistema di gestione della sicurezza delle informazioni della DIGIT CONSULTING definisce un insieme di misure organizzative e tecniche procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- Riservatezza : ovvero la proprietà dell’informazione di essere nota solo a chi ne ha i privilegi;
- Integrità : ovvero la proprietà dell’informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità : ovvero la proprietà dell’informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre con la presente politica, DIGIT CONSULTING intende formalizzare i seguenti obiettivi nell’ambito della sicurezza delle informazioni:

- Preservare al meglio l’immagine dell’azienda quale fornitore affidabile e competente.
- Proteggere il proprio patrimonio informativo.
- Evitare, per quanto possibile, i ritardi nel delivery.

- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità.
- Rispondere pienamente alle indicazioni della normativa vigente e cogente.
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza.

### 2.1.2. Criteri per l'identificazione della tipologia delle informazioni.

DIGIT CONSULTING è consapevole sia dell'importanza della tutela della riservatezza delle informazioni in generale e sia che non tutte le informazioni necessitano dello stesso grado di sicurezza e segretezza del dato. Poiché l'aumento dei livelli di protezione implica un aumento nell'utilizzo di risorse e un conseguente aumento di costi DIGIT CONSULTING ha suddiviso le informazioni in categorie distinte ai quali applica diversi trattamenti. Ogni informazione può appartenere ad una o più categorie.

#### • *Informazioni interne ed esterne.*

- **Interne:** fanno parte di questa categoria tutte le informazioni aziendali associate al personale, alle mansioni, ai ruoli, agli strumenti aziendali necessarie allo svolgimento dell'attività lavorativa quotidiana. Alle informazioni interne afferiscono anche tutti i dati clienti necessari all'erogazione del servizio o ad attività amministrative ad esso associate.
- **Esterne:** fanno parte di questa categoria le informazioni del cliente o di terzi, fornite dal cliente, cui DIGIT CONSULTING viene a conoscenza nell'erogazione del servizio richiesto. A questa categoria appartengono: i documenti e dati utilizzati per il test e il collaudo degli applicativi in licenza; i documenti e dati utilizzati per il debug; i documenti e dati che DIGIT CONSULTING conserva, elabora e gestisce conto terzi nei propri impianti.

#### • *Informazioni identificative aziendali e personali.* –

**Aziendali:** fanno parte di questa categoria le informazioni che identificano o rendono identificabile una persona giuridica (azienda), solitamente sono informazioni pubbliche.

✓ **Personali:** fanno parte di questa categoria le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica. Queste a loro volta possono contenere dati il cui grado di riservatezza sia sensibilmente diverso e sono di tipo:

- **identificativi:** quelli che permettono l'identificazione diretta, come i dati anagrafici;
- **particolari:** quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;
- **giudiziari:** quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o di indagato.

La classificazione e la successiva modalità di trattamento dei dati per le diverse categorie sono indicate nelle procedure e nei documenti del sistema di gestione aziendale e nella documentazione redatta per gli obblighi normativi cui è soggetta la DIGIT CONSULTING riguardo il Regolamento UE 679/2016.

### 2.1.3 Responsabilità

Tutto il personale che a qualsiasi titolo collabora con l'azienda è responsabile dell'osservanza della presente policy, per questo sottoscrive un "accordo alla riservatezza" che lo impegna anche dopo il termine del rapporto contrattuale con la DIGIT CONSULTING ed è tenuto a partecipare alla segnalazione delle anomalie, anche formalmente non codificate, di cui dovesse venire a conoscenza.

Il lavoratore che non rispetti i criteri di policy delle informazioni può essere soggetto a sanzioni disciplinari a seconda della gravità.

Il Comitato di sicurezza è un organo in staff alla direzione che si costituisce su richiesta della Direzione stessa per analizzare situazioni critiche di eventi ed incidenti e/o per redigere linee guida su specifiche attività inerenti la sicurezza delle informazioni.

Il comitato è costituito dal Responsabile IT e RGS.

Responsabile della Sicurezza delle Informazioni che si occupa della progettazione del sistema della Sicurezza delle Informazioni ed in particolare:

- Suggestire le misure di sicurezza organizzative, procedurali, tecnologiche a tutela della sicurezza e per la continuità delle attività in e di DIGIT CONSULTING.
- Controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce.
- Verificare gli incidenti di sicurezza ed adottare le opportune contromisure.

Responsabile del Sistema di Gestione che si occupa di:

- Emanare tutte le norme necessarie ivi inclusa la classificazione e divulgazione dei documenti affinché l'organizzazione aziendale possa condurre in modo sicuro le proprie attività.
- Pianificare per il personale un percorso formativo specifico e periodico in materia di sicurezza.
- Promuovere la cultura relativa alla sicurezza delle informazioni.
- Contribuire alla definizione delle contromisure da adottare a seguito di eventuali incidenti.

La gestione ed il controllo dei rischi per la sicurezza informazioni è parte integrante della governance. In pratica vengono delegate esplicitamente le responsabilità esecutive per la maggior parte delle questioni di governance ai responsabili di funzione, coordinati dall'amministratore unico. Rimangono in capo a quest'ultimo le decisioni per investimenti che abbiano importi per cui sono richiesti poteri di delega specifici e non quindi ricompresi in quelli dei responsabili di funzione.

I Responsabili di funzione coordinano le attività in tutta l'organizzazione, garantendo che le politiche siano le più adatte a sostegno dei principi ed assiomi di sicurezza dell'organizzazione. I Responsabili di Funzione basano le loro attività anche sul feedback del Comitato della Sicurezza e dell'Ufficio Legale per garantire che i principi, gli assiomi e le politiche vengano attuati.

I Responsabili di funzione dimostrano il loro impegno alla sicurezza delle informazioni:

- tramite il sostegno alla Direzione assunto in fase di avvio del sistema e successivamente in fase di Riesame della Direzione in cui sono verificati e riapprovati i principi e assiomi per la sicurezza delle informazioni;
- includendo, se necessari, nel bilancio in fase preventiva specifici accantonamenti per la sicurezza delle informazioni;
- producendo opportuni report sulla gestione per quanto riguarda la sicurezza delle informazioni in merito a metriche di performance, eventi ed incidenti di sicurezza, richieste di investimento e loro stato di attuazione.

L'attività di sicurezza di informazioni viene supervisionata in tutta l'organizzazione al fine di garantire l'applicazione coerente dei principi di sicurezza, gli assiomi e le dichiarazioni politiche.



I Responsabili di funzione sono responsabili:

- dell'applicazione quotidiana della policy di sicurezza informazioni;
- di garantire che opportuni controlli tecnici, fisici e procedurali, in linea con le policy di sicurezza delle informazioni, siano correttamente applicati e utilizzati da tutti i lavoratori. In particolare, dovrebbero adottare misure per garantire che i lavoratori:
- siano informati del loro obbligo di adempiere le dichiarazioni politiche aziendali rilevanti per mezzo di opportune attività di sensibilizzazione, formazione e istruzione;
- rispettino le istruzioni di sicurezza e attivino i controlli associati.
- di fornire le linee operative, risorse ed il supporto necessari affinché le informazioni siano protette in modo appropriato all'interno della loro area di responsabilità;
- di informare il Comitato della Sicurezza sulle violazioni dei criteri effettivi o presunti (incidenti di sicurezza informazioni) che interessano i loro asset e patrimonio informativo;
- di valutare la conformità con gli assiomi di politica attraverso il normale processo di coordinamento delle attività operative e occasionali audit interni.
- della classificazione appropriata e delle indicazioni per la protezione del patrimonio di informazioni;
- di individuare idonei controlli e misure per la protezione del patrimonio informativo e di redigere le opportune valutazioni per i costi necessari alla loro acquisizione;
- di autorizzare la richiesta di accesso alle risorse informative in conformità con la classificazione e le necessità operative della divisione, nel rispetto delle competenze del proprio personale;
- per i nuovi sviluppi di valutare i rischi di sicurezza per garantire che i requisiti di protezione di informazioni siano correttamente definiti e documentati durante le prime fasi di sviluppo;
- di assicurare corretta gestione degli accessi al patrimonio aziendale ed una corretta applicazione per il deprovisioning;
- della verifica della conformità ai requisiti di protezione che interessano i loro beni.

Tutti i soggetti esterni che intrattengono rapporti con DIGIT CONSULTING devono garantire il rispetto dei requisiti della sicurezza esplicitati dalla presente politica di sicurezza anche tramite la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non è espressamente previsto nel contratto.

#### 2.1.4. Applicabilità

La presente politica si applica indistintamente a tutti gli organi dell'azienda. L'attuazione della presente politica è obbligatoria per tutte le risorse di DIGIT CONSULTING, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda. DIGIT CONSULTING consente la comunicazione e diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che avvengono sempre nel rispetto delle regole nonché delle norme e leggi cogenti.

La Direzione