



POL01 - Politica per la Sicurezza delle Informazioni

2024

Versione 01

Revisione:	01
Data Emissione:	07/05/2024
Emesso da:	Responsabile del Sistema di Gestione Integrato
Approvato:	Direzione aziendale



Lista dei cambiamenti

VERSIONE	DATA	DESCRIZIONE	AUTORE
01	07/05/2024	Prima Versione	404



Sommario

Politica per la Sicurezza delle Informazioni	4
Criteri per l'accettazione del rischio e livelli di rischio	7



Politica per la Sicurezza delle Informazioni

Il presente documento definisce la Politica del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) intesa come l'impegno della Direzione per impostare un approccio organizzato alla gestione della sicurezza delle informazioni trattate dall'organizzazione. Le informazioni gestite dal Gruppo 404, nelle loro molteplici forme rappresentano un bene fondamentale e, dato il loro valore, necessitano di essere protette in modo appropriato. A fronte di possibili minacce e vulnerabilità, la sicurezza delle informazioni protegge queste ultime implementando un insieme di controlli che nascono da una corretta e completa attuazione della Politica per la Sicurezza delle informazioni. Infatti, una Politica per la Sicurezza delle Informazioni che rifletta gli obiettivi e i requisiti aziendali, nonché le leggi e i regolamenti pertinenti, che sia sostenuta dalla Direzione e distribuita a tutto il personale coinvolto, contribuisce fortemente ad avviare, attuare, mantenere e migliorare la gestione della sicurezza delle informazioni.

La Politica per la Sicurezza per le risorse incluse nel SGSI è quella di proteggere tali risorse dalle minacce (interne, esterne, deliberate, accidentali) che possono comprometterle. In particolare, per tutti i sistemi sotto SGSI, è necessario assicurare che:

- le informazioni siano accessibili esclusivamente alle persone autorizzate, sia interne sia esterne all'azienda, garantendo livelli di servizio e complessità compatibili con i requisiti funzionali dei sistemi interessati;
- qualunque sia il formato delle informazioni trattate, sia garantita la loro disponibilità, integrità e riservatezza nel rispetto dei requisiti legislativi applicabili;
- sia effettuato un monitoraggio costante nel cambiamento degli asset e della tecnologia al fine di identificare tempestivamente nuove vulnerabilità;
- sia effettuato un costante aggiornamento sui siti specializzati in tematiche di sicurezza e forum per la pronta individuazione di nuove tipologie di minacce;
- sia prestata particolare attenzione alle variazioni dei requisiti normativi, contrattuali ed alle relative priorità in relazione a nuovi sviluppi applicativi;
- sia garantita la continuità operativa attraverso interventi mirati, sia organizzativi sia tecnologici, e che tali interventi siano definiti, costantemente aggiornati e periodicamente verificati;



- tutto il personale sia addestrato sulla sicurezza, che sia informato dell'obbligatorietà delle politiche aziendali in merito e che sia altresì sensibilizzato sulle conseguenze derivanti dalla violazione delle politiche aziendali;
- siano effettuate valutazioni periodiche dell'efficacia del SGSI e della formazione del personale attraverso simulazioni nell'ambito di applicazione (test di penetrazione/intrusione sulla sicurezza logico-fisica, test di conoscenza delle policy e simulazioni di violazioni delle stesse);
- siano introdotte metriche per la valutazione delle prestazioni del sistema;
- siano separate le mansioni relative alle attività critiche (ad esempio sviluppo e collaudo con la produzione);
- siano ridotti il più possibile i rischi alla fonte;
- qualsiasi violazione della sicurezza, reale o presunta, sia comunicata ed investigata;
- siano prontamente identificati e gestiti gli incidenti sulla sicurezza ed attivate le autorità competenti per quelli che hanno impatto su requisiti di legge violati;
- sia evitato l'utilizzo di software non autorizzati;
- siano effettuati riesami periodici del SGSI relativamente a:
 - o verifica dell'attualità e dell'efficacia dei controlli applicati per le minacce e le vulnerabilità individuate nel piano del trattamento dei rischi;
 - o incidenza dei controlli attuati sull'efficacia gestionale;
 - o modifiche apportate dalla tecnologia (vulnerabilità nuove o modificate, riduzione dei rischi per nuove conoscenze acquisite in base al progresso tecnologico);
 - o modifiche apportate alla configurazione dei sistemi sotto SGSI;
 - o rivalutazione periodica del rischio ed in particolare a monte e a valle di qualsiasi azione preventiva.

Al fine di stabilire, attuare, monitorare, aggiornare e migliorare il SGSI, la Direzione si impegna, inoltre, a fornire sufficienti risorse per condurre un'analisi e trattamento dei rischi per la sicurezza delle informazioni. La Direzione, con il sostegno delle risorse individuate:

- identifica una metodologia di valutazione del rischio;
- identifica, analizza e pondera i rischi individuati;



- stabilisce i criteri per l'accettazione dei rischi e i livelli di rischio accettabili;
- seleziona i controlli che devono essere attuati;
- garantisce che siano realizzate le misure di sicurezza identificate nella fase di trattamento dei rischi, attraverso attività di audit, monitoraggio e riesame;
- intraprende azioni preventive e correttive, e si assicura che i miglioramenti conseguano gli obiettivi prefissati.

La responsabilità dell'istituzione e della gestione del SGSI è di competenza della Direzione.

Il SGSI viene riesaminato ogni anno o nel caso si verificano cambiamenti significativi al SGSI stesso. Il riesame del SGSI include un riesame della Politica per la sicurezza delle informazioni. Il riesame della Politica, che necessita dell'approvazione della Direzione, comprende la valutazione delle opportunità di miglioramento della Politica per la sicurezza delle informazioni e dell'esigenza di apportare aggiornamenti in risposta ai cambiamenti dell'ambiente, delle circostanze aziendali, delle condizioni legali o degli aspetti tecnico-organizzativi.

Nello specifico, il riesame della Politica del SGSI tiene conto dei:

- riesami precedenti;
- attività di audit e monitoraggio;
- stato delle azioni preventive e correttive;
- informazioni di ritorno delle parti interessate (personale interno, Utenti, ecc.);
- nuove tecnologie e procedure;
- nuovi scenari di sicurezza in termini di vulnerabilità e minacce;
- report sugli incidenti di sicurezza;
- raccomandazioni e/o obblighi delle Autorità pertinenti.

Il riesame della Politica del SGSI dovrebbe portare ad un miglioramento dell'efficacia del SGSI, dei controlli e della distribuzione delle risorse e delle responsabilità.

Ogni riesame della Direzione è registrato secondo le politiche di registrazioni specificate in apposita documentazione.



Criteri per l'accettazione del rischio e livelli di rischio

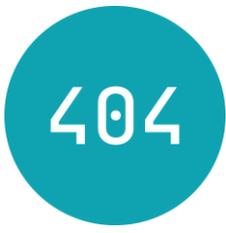
Al fine di allineare la presente politica con il contesto di gestione del rischio strategico dell'organizzazione all'interno del quale avranno luogo l'impostazione e l'aggiornamento del SGSI e per stabilire i criteri con i quali ponderare il rischio, viene di seguito descritta una tabella di valutazione del rischio.

I livelli di rischio definiti indicano i casi in cui può essere compromesso il raggiungimento delle strategie e degli obiettivi del Gruppo 404.

Livello di Rischio	Valutazione
ALTO (INACCETTABILE)	Un rischio è inaccettabile qualora l'impatto abbia un effetto significativo sul raggiungimento degli obiettivi strategici, ad esempio: <ul style="list-style-type: none">• perdita di dati critici;• dati e servizio non disponibili;• perdita o significativa riduzione della credibilità/immagine nei confronti dei portatori di interesse;• sanzioni penali a carico dei dipendenti.
SIGNIFICATIVO	Inefficienza delle normali operazioni con un effetto limitato sul raggiungimento degli obiettivi strategici, ad esempio: <ul style="list-style-type: none">• interruzioni o significative inefficienze nel processo di gestione del servizio;• problemi temporanei di qualità/servizio;• inefficienze nei flussi e nelle operazioni.
ACCETTABILE	Nessun impatto concreto sulla strategia del Gruppo 404. Si tratta di situazioni diverse dalla norma che richiedono comunque azioni correttive.

Questi criteri generali potranno poi essere ulteriormente dettagliati nella specifica attività di valutazione del rischio del SGSI.

Milano 07/05/2024
La Direzione



POL02 - Politica per la Qualità

2024

Versione 01

Revisione:	01
Data Emissione:	07/05/2024
Emesso da:	Responsabile del Sistema di Gestione Integrato
Approvato:	Direzione aziendale



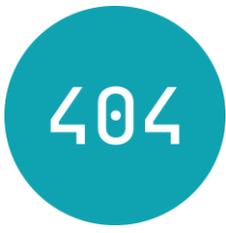
Lista dei cambiamenti

VERSIONE	DATA	DESCRIZIONE	AUTORE
01	07/05/2024	Prima Versione	404



Sommario

Politica per la Qualità 4

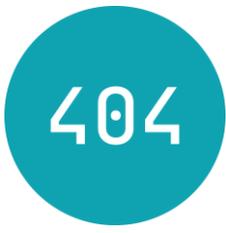


Politica per la Qualità

La Direzione Aziendale ha avviato un processo di diversificazione delle proprie attività e di adeguamento della propria struttura organizzativa aziendale, per assecondare e, ove possibile, anticipare le tendenze del mercato. L'azienda, infatti, impegnata attualmente nel supervisionare e coordinare le attività delle società controllate al fine di massimizzare il valore complessivo del gruppo e garantire il conseguimento degli obiettivi aziendali, ha intrapreso importanti iniziative anche nel campo prettamente tecnologico e informatico, al fine di garantire la massima soddisfazione del cliente. Attualmente il Gruppo 404, oltre alla Società 404, si compone di altre due Società, O&DS e Digital Garage Labs, le attività delle due entità operative controllate sono ascrivibili a servizi di consulenza e realizzazione di progetti e prodotti di information technology e, in particolare, in ambito web e digital.

Obiettivo della Società è fare in modo che tutte le attività siano sviluppate con efficienza ed economicità attivando un sistema di gestione aziendale improntato sui seguenti principi fondamentali:

- rispetto dei requisiti contrattuali, continuo miglioramento del prodotto e del servizio reso nell'ottica di accrescere la soddisfazione del cliente mediante l'erogazione del miglior livello di servizio possibile;
- costante determinazione nella ricerca ed eliminazione delle "Non Conformità" al fine di garantire il miglioramento continuo dei processi;
- sviluppo continuo delle proprie competenze, per svolgere verso i clienti un ruolo propositivo in modo da anticipare le necessità e le sfide del loro mercato;
- valorizzazione del know-how aziendale e del patrimonio professionale "personale";
- predisposizione di un sistema di gestione delle risorse umane che garantisca lo sviluppo e l'evoluzione delle competenze necessari;
- perseguimento di uno spirito di collaborazione con i Fornitori allo scopo di attivare rapporti improntati ad una crescita continua e congiunta della qualità complessiva offerta al mercato;
- rispetto delle leggi vigenti in materia di sicurezza, di igiene del lavoro, antinfortunistica e di tutela dell'ambiente;
- valutazione periodica dei risultati e delle decisioni aziendali sui dati forniti dagli indicatori relativi alla soddisfazione del cliente, alla qualità dei prodotti forniti, all'efficienza dei processi, compresi i risultati economici dell'azienda.



A tal fine, sin dalla nascita dell'azienda, la Direzione ha avviato un processo di miglioramento continuo della struttura organizzativa e dei processi aziendali per assecondare e, ove possibile, anticipare le tendenze e le esigenze del mercato.

In quest'ottica, la Direzione, consapevole del proprio ruolo di leadership, considera la Qualità un elemento cardine della propria strategia e promuove l'impegno per la qualità a tutti i livelli dell'organizzazione.

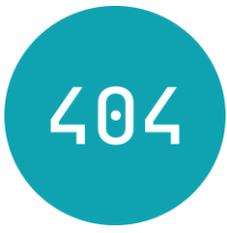
Proprio per tale motivo, il Gruppo 404 ha deciso, a partire dal 2024, di implementare un Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni in conformità alla versione della norma UNI EN ISO 9001:2015 e ISO/IEC 27001:2022.

Al fine di garantire la qualità dei propri servizi il Gruppo 404 ha messo in campo iniziative quali:

- Mantenimento e applicazione di un Sistema di gestione per la qualità efficacemente gestito, tale da garantire gli obiettivi di:
 - o soddisfazione del cliente;
 - o qualità dei prodotti forniti;
 - o approccio alla qualità nell'ottica del *risk based thinking*;
 - o efficienza interna.
- Mantenimento e applicazione di un sistema di monitoraggio e di riesame dei risultati per garantire il controllo sistematico, con attuazione del miglioramento.
- Gestione delle risorse basata su politiche di sviluppo delle capacità, competenze tecniche per la progettazione e per l'innovazione.

Per garantire l'attuazione di tali iniziative, la Direzione definisce annualmente un Piano di Obiettivi per la qualità allo scopo di ottenere:

- Monitoraggio e analisi dei dati dei vari processi aziendali;
- Monitoraggio e misura della soddisfazione del Cliente;
- Miglioramento del Sistema di Gestione per la Qualità;
- Formazione per la qualità del personale (informazione, coinvolgimento, formazione).



La Direzione del Gruppo 404 fa presente che il conseguimento degli obiettivi sopra definiti è una responsabilità di tutto il personale e coinvolge quindi ogni funzione aziendale nell'ambito dei compiti assegnati.

Milano 07/05/2024
La Direzione