

# POLITICA DEL SISTEMA DI GESTIONE DEI SERVIZI (SGS)

## Edizione del Documento

Codice documento:	POLITICA DEL SISTEMA DI GESTIONE DEI SERVIZI (SGS)
Versione:	Prima emissione
Data della versione:	03/06/2024
Redatto da:	Dario Parodi
Approvato da:	Direzione
Classificazione documento:	Di uso esclusivo di ufficio

## Storia dei cambiamenti

Data	Versione	Redatto da	Descrizione del cambiamento
03/06/2024	1	Dario Parodi Alessandro Feltrin	Rielaborazione del documento "IMPEGNO POLITICA AUTORITA' E CAMPO DI APPLICAZIONE" Pr. 02 Rev. 05 del 30.12.2022 scorporando il contesto relativo a quanto di interesse della norma ISO 20000-1:2018
30/11/2025	1.1	Dario Parodi	Revisione generale

## SOMMARIO

1. SCOPO	3
2. AMBITO DI APPLICAZIONE	3
3. PRINCIPI DEL SISTEMA DI GESTIONE DEI SERVIZI	3
4. PIANO STRATEGICO E OBIETTIVI DEL SGS	4
4.1. OBIETTIVI STRATEGICI	4
4.2. OBIETTIVI OPERATIVI	4
5. RUOLI E RESPONSABILITÀ	5
5.1. DIREZIONE AZIENDALE	5
5.2. RESPONSABILE DEL SISTEMA DI GESTIONE INTEGRATO	5
5.3. RESPONSABILE DEI SISTEMI	5
5.4. TEAM IT E OPERATIONS	5
5.5. RESPONSABILE DELLA SICUREZZA IT	5
5.6. RESPONSABILE DELLA CONTINUITÀ OPERATIVA	5
5.7. UTENTI E CLIENTI	6
6. REVISIONE E AGGIORNAMENTO	6

Di uso esclusivo d'ufficio

## 1. SCOPO

Questa politica stabilisce i principi e gli obiettivi del **Sistema di Gestione dei Servizi (SGS)** implementato da **N&C**, in conformità con i requisiti della norma **ISO/IEC 20000-1:2018**.

L'obiettivo principale è garantire la fornitura di servizi IT di alta qualità, affidabili e orientati alle esigenze dei clienti e delle parti interessate.

## 2. AMBITO DI APPLICAZIONE

Il **SGS di N&C** si applica a tutti i servizi IT forniti ai clienti interni ed esterni, inclusi:

- **Sviluppo software** e gestione del ciclo di vita delle applicazioni.
- **Gestione e manutenzione degli applicativi IT.**
- **Gestione delle infrastrutture di rete e dei data center.**
- **Sicurezza IT e protezione delle informazioni.**
- **Supporto IT e Service Desk.**
- **Business Continuity & Disaster Recovery.**

Inoltre, questa politica si applica a tutto il personale, ai fornitori e ai partner coinvolti nella fornitura dei servizi.

## 3. PRINCIPI DEL SISTEMA DI GESTIONE DEI SERVIZI

Per garantire un'efficace gestione dei servizi IT, l'azienda si impegna a rispettare i seguenti principi:

- **Orientamento al Cliente**
  - Assicurare che i servizi IT soddisfino i requisiti contrattuali e le esigenze dei clienti.
  - Implementare un processo continuo di gestione delle richieste e dei feedback.
  - Monitorare regolarmente la soddisfazione del cliente e migliorare i servizi in base ai risultati.
- **Efficienza Operativa e Qualità del Servizio**
  - Garantire un livello di servizio (SLA) ottimale, rispettando tempi e performance stabilite.
  - Implementare un monitoraggio continuo delle prestazioni dei servizi.
  - Adottare processi di miglioramento continuo basati su dati e analisi.
- **Compliance e Conformità**
  - Rispettare i requisiti della ISO/IEC 20000-1:2018.
  - Assicurare la conformità alle normative di sicurezza IT (ISO 27001) e privacy (GDPR).
  - Adottare un approccio strutturato per la gestione dei rischi.
- **Continuità Operativa e Sicurezza**
  - Implementare piani di Business Continuity e Disaster Recovery.

## SIG-ISO 20000-POL-5.2 - POLITICA DEL SISTEMA DI GESTIONE DEI SERVIZI (SGS)

- Proteggere i dati aziendali e dei clienti tramite misure di cybersecurity avanzate.
- Garantire la disponibilità e l'integrità dei servizi anche in caso di incidenti.
- **Miglioramento Continuo**
  - Adottare metodologie ITIL per ottimizzare la gestione dei servizi.
  - Effettuare audit interni periodici per garantire il rispetto della ISO 20000.
  - Promuovere la formazione e lo sviluppo del personale IT.

## 4. PIANO STRATEGICO E OBIETTIVI DEL SGS

Per garantire l'efficacia e l'efficienza del SGS, l'organizzazione ha definito un piano strategico basato sui seguenti obiettivi:

### 4.1. OBIETTIVI STRATEGICI

- **Allineamento con le esigenze aziendali e dei clienti:** Assicurare che i servizi IT supportino gli obiettivi aziendali e le esigenze operative dei clienti attraverso un processo continuo di raccolta dei requisiti e analisi delle prestazioni.
- **Miglioramento continuo:** Applicare il ciclo PDCA (Plan-Do-Check-Act) per ottimizzare la gestione dei servizi IT, con audit periodici e analisi delle cause radice per l'identificazione delle aree di miglioramento.
- **Innovazione e trasformazione digitale:** Adottare nuove tecnologie e metodologie, come DevOps, ITIL e automazione, per migliorare la qualità e la scalabilità dei servizi IT.
- **Gestione dei rischi IT:** Identificare, valutare e mitigare i rischi attraverso analisi periodiche, simulazioni di attacco informatico e piani di continuità operativa.
- **Soddisfazione del cliente:** Monitorare il livello di soddisfazione attraverso sondaggi periodici, gestione dei reclami e miglioramenti basati sul feedback ricevuto.
- **Sostenibilità e responsabilità sociale:** Implementare pratiche IT eco-sostenibili, ridurre i consumi energetici e favorire l'adozione di tecnologie a basso impatto ambientale.

### 4.2. OBIETTIVI OPERATIVI

- **Migliorare i tempi di risposta agli incidenti IT:** Ridurre il tempo medio di risoluzione (MTTR) degli incidenti critici entro [X] ore, attraverso strumenti avanzati di monitoraggio e automazione dei processi.
- **Aumentare l'affidabilità dei servizi IT:** Mantenere un uptime minimo del [99.X]% per i servizi critici, utilizzando strategie di alta disponibilità e ridondanza.
- **Potenziare la sicurezza IT:** Implementare misure di cybersecurity avanzate, tra cui firewall di nuova generazione, autenticazione multi fattore e analisi del traffico di rete, per ridurre il numero di violazioni della sicurezza.
- **Gestione efficace delle modifiche:** Applicare procedure di Change Management strutturate per ridurre gli impatti negativi derivanti dalle modifiche non pianificate ai servizi IT.

## SIG-ISO 20000-POL-5.2 - POLITICA DEL SISTEMA DI GESTIONE DEI SERVIZI (SGS)

- **Formazione e consapevolezza:** Garantire che il personale IT e gli utenti finali ricevano una formazione continua sulla gestione dei servizi IT, inclusi corsi su best practice, sicurezza informatica e conformità normativa.
- **Ottimizzazione dei costi IT:** Razionalizzare le spese IT attraverso un'accurata gestione delle risorse, valutazione dei fornitori e ottimizzazione degli investimenti tecnologici.
- **Miglioramento della gestione della configurazione:** Assicurare un efficace Configuration Management per mantenere un inventario aggiornato delle risorse IT e ridurre gli impatti delle modifiche.
- **Adozione di standard di interoperabilità:** Favorire l'adozione di framework e API standardizzati per migliorare l'integrazione tra sistemi e ridurre la complessità gestionale.

## 5. RUOLI E RESPONSABILITÀ

### 5.1. DIREZIONE AZIENDALE

- Definisce e approva la strategia del SGS.
- Assegna risorse per l'implementazione e il miglioramento continuo del SGS.
- Garantisce che il SGS sia allineato con gli obiettivi aziendali e di conformità.
- Valuta periodicamente l'efficacia del SGS attraverso audit e revisioni di performance.

### 5.2. RESPONSABILE DEL SISTEMA DI GESTIONE INTEGRATO

- Coordina l'implementazione e il mantenimento del SGS.

### 5.3. RESPONSABILE DEI SISTEMI

- Supervisiona le attività di gestione dei servizi IT e delle prestazioni.
- Monitora la conformità ai requisiti della ISO 20000-1 e promuove miglioramenti.
- Gestisce la comunicazione tra i vari stakeholder coinvolti nel SGS.

### 5.4. TEAM IT E OPERATIONS

- Implementa e segue le procedure definite dal SGS.
- Gestisce la risoluzione degli incidenti, problemi e cambiamenti secondo gli SLA.
- Garantisce l'aggiornamento della documentazione del SGS.
- Contribuisce al miglioramento continuo attraverso il feedback e l'analisi delle prestazioni.

### 5.5. RESPONSABILE DELLA SICUREZZA IT

- Supervisiona la protezione dei dati e delle infrastrutture IT.
- Coordina le attività di cybersecurity per la gestione delle minacce e delle vulnerabilità.
- Collabora con il team SGS per garantire la resilienza dei servizi IT.

## 5.6. RESPONSABILE DELLA CONTINUITÀ OPERATIVA

In azienda il ruolo è ricoperto dal Responsabile del Sistema di Gestione Integrato (RSGI)

L'RSGSI si coordina con il CTO, con Il responsabile della Sicurezza IT e con il Responsabile dei Sistemi per

- Pianificare e testare regolarmente i piani di continuità e ripristino dei servizi IT.
- Assicurare che i piani di emergenza siano aggiornati e adeguati ai potenziali rischi.
- Coordinare le azioni di risposta in caso di eventi critici che possano compromettere i servizi IT.

## 5.7. UTENTI E CLIENTI

- Forniscono feedback sulle prestazioni dei servizi IT.
- Segnalano eventuali problemi o disservizi attraverso i canali di supporto.
- Collaborano nel rispetto delle procedure e delle politiche di sicurezza.

## 6. REVISIONE E AGGIORNAMENTO

Questa politica viene revisionata almeno **una volta all'anno** o in caso di cambiamenti significativi nei servizi IT o nelle normative. Le revisioni vengono approvate dalla **Direzione IT** e dal **Responsabile del SGS**.