POLITICA PER LA QUALITÀ E DI SICUREZZA DELLE INFORMAZIONI

Attribuzione del documento

Copia n° **1**

Nome Destinatario **Patrizia Belluomo**

Qualifica **RGSI (Copia in visione a tutto il personale)**

Modifiche e Revisioni

Rev.	Data	Descrizione della modifica
00	11/01/2016	Prima emissione
01	11/01/2017	Revisione per NC 03 del 15-16/12/2016
02	16/01/2018	Revisione Riesame della Direzione del 16/01/2018
03	16/11/2022	Revisione per eliminazione servizio mailing list
04	25/10/2023	Revisione per aggiornamento annuale definizioni e riferimenti

Emissione, Verifica ed approvazione

Emissione a cura di	**Resp Servizio**	**Salvatore Monforte**
Verifica a cura di	**RGSI**	**Patrizia Belluomo**
Approvazione a cura di	**Resp Servizio**	**Salvatore Monforte**

INDICE

1. INTRODUZIONE 4
2. SCOPO E CAMPO DI APPLICAZIONE 4
2.1 Scopo 4
2.2 Campo di applicazione e destinatari 4
2.2.1 Comunicazione 5
2.2.2 Revisione e controllo 5
3. OBIETTIVI 5
4. DEFINIZIONI E ABBREVIAZIONI 6
5. RIFERIMENTI 7
6. DICHIARAZIONE DI PRINCIPIO 8
7. POLICY SPECIFICHE DI SICUREZZA DELLE INFORMAZIONI 9
7.1 Uso dei sistemi di elaborazione delle informazioni 9
7.1.1 Verifiche di sicurezza e controlli delle strumentazioni 9
7.2 Organizzazione e responsabilità della sicurezza delle informazioni 9
7.2.1 Obiettivi 9
7.2.2 Generalità 9
7.2.3 Responsabilità 10
7.3 Scambio di informazioni 10
7.3.1 Obiettivi 10
7.3.2 Flussi di informazioni con altre organizzazioni 10
7.4 Gestione dei rischi 11
7.4.1 Obiettivi 11
7.4.2 Interruzione dei servizi 11
7.4.3 Accessi non autorizzati 11
7.4.4 Qualità dei dati 11
7.4.5 Furti informatici 11
7.4.6 Software malevolo (virus, trojan, ecc.) 11
7.5 Trattamento dei dati 11
7.6 Continuità operativa 12
7.6.1 Obiettivi 12
7.6.2 Requisiti per l'operatività 12
7.6.3 Elementi di pianificazione 12
7.7 Inventario delle risorse 12
7.7.1 Obiettivi 12
7.7.2 Inventario 12
7.7.2.1 Inventario risorse fisiche 12
7.7.2.2 Inventario risorse hardware 13
7.7.2.3 Inventario risorse software 13
7.8 Sicurezza fisica ed ambientale 13
7.8.1 Obiettivi 13
7.8.2 Sicurezza delle aree 13
7.8.3 Sicurezza dei locali 13
7.8.4 Controllo degli accessi ai locali 13
7.9 Sicurezza logica 13
7.9.1 Obiettivi 13
7.9.2 Accesso ai sistemi ed alle applicazioni 14
7.9.2.1 Regole di accesso 14
7.9.2.2 Accesso alla rete 14
7.9.2.3 Accesso alle applicazioni 14
7.9.2.4 Caratteristiche e gestione delle password 14
7.9.3 Utilizzo e gestione del software 15
7.9.3.1 Gestione software su licenza 15

7.9.3.2 Sviluppo di applicazioni software.....15
7.10 Backup dei dati ed uso dei dispositivi di memorizzazione.....15
7.11 Sicurezza delle reti delle telecomunicazioni.....15
7.12 Gestione degli incidenti informatici.....16

1. INTRODUZIONE

Il *Servizio Calcolo e Reti dell'INFN Sezione di Catania* (di seguito *Servizio Calcolo e Reti*) ha implementato un Sistema Gestionale Integrato (SGI) per la qualità (SGQ) e per la sicurezza delle informazioni (SGSI) conforme alle norme UNI EN ISO 9001:2015 ed UNI CEI ISO/IEC 27001:2014.

Il *Servizio Calcolo e Reti* durante le l'*attività* di *Gestione di reti cablate e wireless, servizi VPN, servizi generali (posta elettronica, server Windows, pagine web utenti) e servizi di calcolo e storage dati (sia fisici che virtuali) attraverso il proprio data center* è impegnato in un processo continuo finalizzato al conseguimento di obiettivi di qualità e di sicurezza delle informazioni di livello sempre più elevato. Ogni funzione interna è impegnata a soddisfare costantemente le esigenze esplicite ed implicite di tutti gli utenti, i servizi erogati e le attività svolte da ciascuno devono conformarsi sempre e totalmente ai requisiti prescritti.

La presente Politica per la Qualità e di Sicurezza delle Informazioni del *Servizio Calcolo e Reti* è stabilità ed attuata per soddisfare i requisiti applicabili delle norme di riferimento, proteggere, per quanto possibile e comunque ad un livello ottimale e ad un costo compatibile con le specificità dell'organizzazione, il proprio SGI, da eventi intesi come minacce o incidenti, esterni e/o interni, oggettivi e/o soggettivi, che possano compromettere l'erogazione dei servizi nonché la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati e delle informazioni gestite.

2. SCOPO E CAMPO DI APPLICAZIONE

2.1 Scopo

Lo scopo del presente documento è quello di descrivere la Politica per la Qualità e di Sicurezza delle Informazioni appropriate alle finalità del contesto dell'organizzazione. Il presente documento viene redatto quale supporto agli indirizzi strategici della Direzione e costituisce un quadro di riferimento per fissare gli obiettivi.

Il Servizio Calcolo e Reti considera il proprio SGI, per il particolare rilievo che ha assunto per il perseguimento dei propri fini istituzionali, parte integrante del proprio patrimonio. E' obiettivo di assoluta priorità per il Servizio Calcolo e Reti, garantire il miglioramento continuo della qualità dei servizi erogati e salvaguardare la sicurezza del proprio sistema informativo e tutelarne la riservatezza, l'integrità, l'autenticità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

In tale contesto si intende per:

Miglioramento continuo:	Attività ricorrente per accrescere le prestazioni

e nell'ambito della sicurezza delle informazioni:

Riservatezza:	la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati.
Integrità:	la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico e sia stata modificata in modo legittimo da soggetti autorizzati.
Disponibilità:	la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura.
Autenticità:	la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

Il *Servizio Calcolo e Reti* pone a base della propria Politica per la Qualità e di Sicurezza delle Informazioni, una idonea analisi delle minacce e delle opportunità di tutte le risorse che costituiscono il proprio SGSI, al fine poterne cogliere i vantaggi per il miglioramento continuo e di comprendere le possibili vulnerabilità, valutare le minacce e di predisporre le necessarie contromisure. La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della propria Politica per la Qualità e di Sicurezza delle Informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un SGSI.

2.2 Campo di applicazione e destinatari

Il documento redatto comprende l'impegno a soddisfare tutti i requisiti applicabili e l'impegno per il miglioramento continuo del SGI.

La presente Politica per la Qualità e di Sicurezza delle Informazioni è valida per l'erogazione dei servizi di *Gestione di reti cablate e wireless, servizi VPN, servizi generali (posta elettronica, server Windows, pagine web utenti) e servizi di calcolo e storage dati (sia fisici che virtuali) attraverso il proprio data center e le proprie strutture di governo* che il *Servizio Calcolo e Reti* eroga ai propri utenti, comprende l'impegno a soddisfare tutti i requisiti applicabili e l'impegno per il miglioramento continuo del SGI, si applica ai processi e alle attività relative all'erogazione dei servizi e alle informazioni trattate nell'ambito prima definito, qualsiasi natura e forma esse abbiano o prendano e a tutti i sistemi di gestione e supporti utilizzati per il loro trattamento e conservazione.

La Politica di Sicurezza delle Informazioni integra quanto prescritto all'interno dei documenti del gruppo Harmony, emessi dalla CCR.

I destinatari della presente Politica per la Qualità e di Sicurezza delle Informazioni sono i dipendenti del *Servizio Calcolo e Reti* e i fruitori dei servizi erogati ovvero dipendenti, associati, convenzionati, visitatori, ospiti e fornitori.

2.2.1 Comunicazione

La Direzione del *Servizio Calcolo e Reti* cura la diffusione al suo interno della presente Politica per la Qualità e di Sicurezza delle informazioni a tutto il personale mediante affissione di una copia aggiornata delle linee guida all'interno di uno spazio accessibile a tutte le funzioni organizzative e la diffusione a tutte le parti interessate mediante l'inserimento della stessa all'interno della pagina web del *Servizio Calcolo e Reti*.

La Direzione si impegna, altresì, attraverso specifici momenti di formazione al proprio personale, affinché la presente politica sia compresa e condivisa da tutto il personale.

2.2.2 Revisione e controllo

La Direzione del *Servizio Calcolo e Reti* è responsabile della revisione periodica della presente Politica per la Qualità e di Sicurezza delle Informazioni affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nel SGI, nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni ed ai contenuti dei documenti del progetto Harmony, emessi dalla CCR.

La presente Politica per la Qualità e di Sicurezza delle Informazioni viene riesaminata ed eventualmente sottoposta a revisione almeno una volta all'anno in occasione del periodico riesame da parte della direzione ovvero in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per il SGI.

3. OBIETTIVI

Il *Servizio Calcolo e Reti* intende continuare ad innalzare e standardizzare la qualità dei propri servizi, al fine di soddisfare nel miglior modo possibile le esigenze degli utenti e di raggiungere la propria piena soddisfazione, garantendo il rispetto di quei valori di riferimento che ne hanno caratterizzato l'azione in termini di etica, moralità, trasparenza, professionalità, investendo nella formazione e fornendo motivazioni per svolgere bene il proprio lavoro.

Nell'ambiente della ricerca, quale è quello in cui il *Servizio Calcolo e Reti* opera, tali principi sono considerati, dalla Direzione, parte integrante delle strategie messe in atto per garantire un adeguato livello di efficienza dei sevizi resi all'interno del contesto in cui opera.

Un punto saliente per le strategie del *Servizio Calcolo e Reti* è la sicurezza delle informazioni trattate e gestite, garantita da un sistema gestionale che ha come punto di partenza il pieno rispetto dei requisiti della normativa cogente.

È ferma convinzione del *Servizio Calcolo e Reti* che la revisione delle procedure di gestione e controllo di tutto il sistema organizzativo garantisca un ambiente di lavoro sereno ed efficiente.

A tale scopo cui il *Servizio Calcolo e Reti* ha prima identificato i seguenti processi principali:

- pianificazione ed erogazione dei servizi;
- gestione dei controlli sui servizi erogati;
- approvvigionamento di beni e servizi;
- miglioramento continuo.

E successivamente definito i seguenti obiettivi generali finalizzati a garantire l'impegno a soddisfare tutti i requisiti applicabili e l'impegno per il miglioramento continuo del SGI:

- ottimizzare e razionalizzare i processi di erogazione dei servizi perseguendo l'efficienza e la sicurezza e garantendo un elevato standard di qualità nei controlli;
- garantire la conformità dei processi e dei servizi erogati ai requisiti cogenti e ai requisiti specificati;
- garantire l'efficacia del sistema gestionale integrato e la sicurezza delle informazioni;
- garantire la soddisfazione degli utenti relativamente alla qualità e alla conformità dei processi e dei servizi erogati;

Per soddisfare tali obiettivi il *Servizio Calcolo e Reti* s'impegna a:

- tenere sotto controllo tutti i processi, identificando ogni problema e gestendo gli scostamenti dagli standard previsti attraverso adeguate azioni correttive e verificandone l'attuazione;
- fornire agli utenti, ai fornitori ed alle terze parti interessate esaurienti e credibili informazioni sui servizi resi e sulle attività svolte.
- garantire al personale una adeguata conoscenza e grado di consapevolezza dei problemi connessi con la sicurezza delle informazioni, al fine di acquisire sufficiente coscienza delle loro responsabilità in merito al trattamento;
- accertare che i fornitori esterni, che svolgono attività con impatto sulla qualità e sulla sicurezza delle informazioni, abbiano consapevolezza delle problematiche di sicurezza delle informazioni del *Servizio Calcolo e Reti* e rispettino la politica adottata dall'organizzazione;
- stabilire le linee guida per l'applicazione di standard, procedure e sistemi per la gestione della sicurezza delle informazioni, garantendo che tutto il personale e tutte le terze parti interessate abbiano consapevolezza delle regole tecniche ed organizzative nell'utilizzo dei sistemi informativi;

Per fare ciò la Direzione garantisce l'informazione, la sensibilizzazione e il coinvolgimento costante tutto il personale attraverso opportuni interventi mirati a rafforzare la competenza e la consapevolezza, così da renderlo non solo partecipe, ma soggetto principale. La Direzione si impegna inoltre a riesaminare ed adeguare costantemente tutto il Sistema Gestionale Integrato e la documentazione ad esso collegata, compresa la presente Politica, ponendosi sempre nuovi obiettivi da raggiungere.

Gli obiettivi generali enunciati nel presente documento vengono tradotti operativamente con frequenza almeno annuale in obiettivi di dettaglio ed indicatori relativi all'efficacia dei processi individuati, garantendo la misurabilità degli sforzi che l'organizzazione si propone di effettuare nel tempo.

Gli obiettivi di dettaglio relativi ai processi individuati, gli indicatori, le azioni da attuare, le risorse da dedicare e le relative responsabilità, i tempi entro i quali raggiungerli e i metodi di misurazione degli indicatori vengono riportati all'interno dei periodici verbali di riesame della direzione.

4. DEFINIZIONI E ABBREVIAZIONI

Sistema Gestionale integrato (SGI)	Sistema Gestionale Integrato conforme alle norme UNI EN ISO 9001:2015 (Sistema di Gestione per la Qualità - SGQ) e UNI CEI ISO/IEC 27001:2014 (Sistema di Gestione della Sicurezza delle Informazioni - SGSI)
CCR	Commissione Nazionale Calcolo e Reti dell'INFN
Direttore di Sezione	Direttore INFN - Sezione di Catania
Resp Servizio	Responsabile del Servizio
RGSI	Responsabile Gestione Sistema Integrato
AA	Addetto Acquisti
CO	Coordinatore Operativo
OP	Operatore
RSI	Referente Sicurezza Informatica

5. RIFERIMENTI

UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità – Requisiti.

UNI CEI ISO/IEC 27001:2014 -Tecnologie informatiche – Sistemi di Gestione per la sicurezza delle informazioni – Requisiti.

Regolamenti posti alla base del SGI e della Politica di Sicurezza delle Informazioni:

- Documenti del progetto "Harmony – linee guida per la sicurezza informatica" emanati dalla CCR e consultabili nel sito internet "https://web.infn.it/CCR/index.php/sito-utenti-del-calcolo/sicurezza-informatica/56-progetti-dei-gruppi-di-lavoro/documentazione-progetti/81-documenti-progetto-harmony" comprendenti:
  - Carta della sicurezza informatica;
  - Norme generali per l'accesso e l'uso delle risorse informatiche;
  - Windows Base;
  - Windows avanzato;
  - Sicurezza MAC;
  - UNIX/LINUX Host Security;
  - Servizi centralizzati;
  - La gestione degli incidenti informatici;
  - Strumento per la sicurezza della LAN;
  - Firewall e Router;
- Documenti del progetto "Harmony – note per l'attuazione delle misure antiterrorismo" emanati dalla CCR e consultabili nel sito internet https://web.infn.it/CCR/index.php/sito-utenti-del-calcolo/sicurezza-informatica/56-progetti-dei-gruppi-di-lavoro/documentazione-progetti/82-documenti-harmony-antiterrorismo comprendenti:
  - Informativa sul trattamento dei dati personali;
  - Condizioni d'uso delle risorse informatiche dell'INFN

Per tutte le norme e/o regolamenti applicabili al SGI si fa riferimento al documento informatico del SGSI modulo F01 Elenco documenti controllati custodito ed aggiornato da RGSI.

6. DICHIARAZIONE DI PRINCIPIO

Politica per la Qualità e di Sicurezza delle informazioni

Il *Servizio Calcolo e Reti* è impegnato in un processo continuo finalizzato al conseguimento di obiettivi di qualità e di sicurezza delle informazioni di livello sempre più elevato. Ogni funzione è impegnata a soddisfare costantemente le esigenze esplicite ed implicite di tutti gli utenti.

I servizi e le attività svolte da ciascuno devono sempre e totalmente conformarsi ai requisiti prescritti garantendo la qualità dei servizi e la protezione delle risorse informative da tutte le minacce, siano esse organizzative o tecnologiche, interne o esterne, accidentali o intenzionali.

I princìpi che stanno alla base della Politica per la qualità e di sicurezza delle informazioni del *Servizio Calcolo e Reti* sono i seguenti:

- correttezza, intesa come rispetto delle aspettative degli utenti, delle parti interessate e degli impegni presi;
- serietà, intesa come affidabilità:
  - dei servizi erogati;
  - delle modalità operative;
  - della sicurezza delle informazioni gestite e trattate attraverso tutte le fasi di erogazione dei servizi;
- conformità, intesa come rispetto dei requisiti legislativi, tecnici e delle norme di riferimento in materia di sicurezza delle informazioni;
- miglioramento, inteso come capacità di porsi e di raggiungere nuovi obiettivi.

Il *Servizio Calcolo e Reti* intende perseguire tali principi affermando con tutte le proprie forze l'immagine di un organizzazione che svolge l'attività di *Gestione di reti cablate e wireless, servizi VPN, servizi generali (posta elettronica, server Windows, pagine web utenti) e servizi di calcolo e storage dati (sia fisici che virtuali) attraverso il proprio data center* nel rigoroso rispetto dell'impegno di fornire servizi rispondenti pienamente ai requisiti richiesti dagli utenti nel rispetto delle norme cogenti garantendo la riservatezza, l'integrità la disponibilità e l'autenticità delle informazioni trattate e gestite.

Il Responsabile del *Servizio Calcolo e Reti*

7. POLICY SPECIFICHE DI SICUREZZA DELLE INFORMAZIONI

7.1 Uso dei sistemi di elaborazione delle informazioni

Il *Servizio Calcolo e Reti* considera i sistemi di elaborazione delle informazioni da lui gestiti, come strumenti di lavoro ed il loro uso, da parte di coloro che vi operano, a qualunque livello e a qualsiasi rapporto, è regolato dallo specifico documento emanato dalla CCR e facente parte del "Progetto Harmony - linee guida per la sicurezza informatica" denominato "Carta della sicurezza informatica".

Gli strumenti messi a disposizione devono essere utilizzati per lo svolgimento dell'attività lavorativa in modo strettamente pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi stessi e della rete, e tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.

Conformemente alle regole del documento "Norme generali per l'accesso e l'uso delle risorse informatiche" le risorse di calcolo ed i servizi di rete sono risorse essenziali che l'INFN mette a disposizione esclusivamente per il conseguimento delle proprie finalità di ricerca scientifica e tecnologica. Il contributo di tutti gli utenti autorizzati a servirsene è fondamentale affinché ne venga preservata la integrità ed il buon funzionamento.

Sono pertanto vietate:

- attività contrarie alle leggi o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
- attività commerciali non autorizzate;
- attività comunque idonee a compromettere la sicurezza delle risorse o dirette a cagionare danni a terzi.

L'INFN promuove un atteggiamento collaborativo fra i soggetti e raccomanda il rispetto di civili consuetudini di comportamento della "netiquette".

Ogni condotta contraria a norme di legge o posta in essere in violazione dei contenuti del documento "Norme generali per l'accesso e l'uso delle risorse informatiche", oltre a produrre eventuali conseguenze penali, civili o disciplinari, determinerà la sospensione dell'accesso alle risorse informatiche stesse previa informazione a Dir Sezione.

7.1.1 Verifiche di sicurezza e controlli delle strumentazioni

Per verificare il corretto utilizzo di tutte le strumentazioni informatiche messe a disposizione degli utenti, il *Servizio Calcolo e Reti* attua quanto stabilito nei documenti emanati dalla CCR e facenti parte del progetto "Harmony – linee guida per la sicurezza informatica". Inoltre, la procedura di controllo del processo PCP01 ai punti 5.1.5, 5.2.4, 5.3.4, 5.4.4, 5.5.4, 5.6.4 e 5.7.4 descrive le attività di valutazione periodica delle vulnerabilità.

7.2 Organizzazione e responsabilità della sicurezza delle informazioni

E' relativa all'individuazione delle procedure dirette alla gestione e controllo delle misure di sicurezza delle informazioni adottate e si concretizza nell'individuazione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del SGI.

7.2.1 Obiettivi

Assicurare che il personale del *Servizio Calcolo e Reti*, in una visione che la sicurezza delle informazioni è una responsabilità comune, sia adeguatamente informato e formato sul ruolo che può svolgere al fine di minimizzare i rischi derivanti dalle minacce alla sicurezza delle informazioni.

7.2.2 Generalità

In accordo con quanto descritto nello specifico documento emanato dalla CNCR e facente parte del "Progetto Harmony - linee guida per la sicurezza informatica" denominato "Carta della sicurezza informatica" l'articolazione organizzativa in ciascuna Sezione prevede la seguente organizzazione:

- il *Direttore di Sezione*, cui compete la responsabilità di assicurare il funzionamento scientifico, organizzativo ed amministrativo della Sezione nel rispetto degli indirizzi approvati dal Consiglio Direttivo; egli è individuato, con

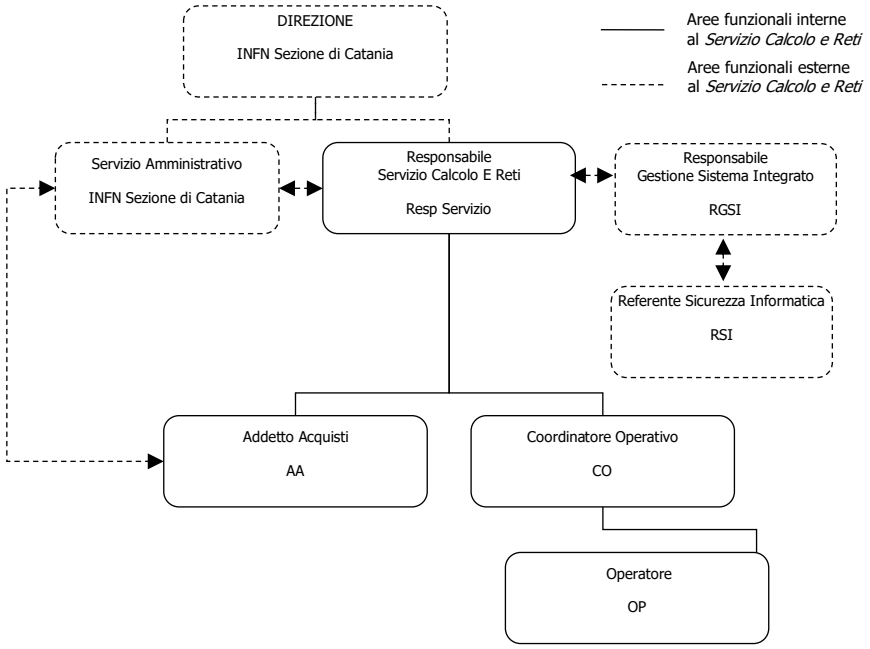
riferimento al trattamento dei dati personali, Responsabile del trattamento ai sensi dell'art. 29 del D.Lgs. 196/03 e successive modificazioni;

- il *Servizio Calcolo e Reti*, cui competono la gestione delle risorse di calcolo centrali, i collegamenti in rete all'interno ed all'esterno della Sezione, nonché la cura, l'installazione e lo sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa di calcolo comunque afferente alla propria Sezione; nell'ambito di ciascun *Servizio Calcolo e Reti* è individuato almeno un referente per i Computer Security Incident Response Team (CSIRT);
- l'*Amministratore di sistema*, con il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione;
- gli *Utenti*, quali soggetti che hanno accesso alle risorse di calcolo e ai servizi di rete, in relazione alle funzioni ed attività che sono chiamati a svolgere nell'ambito dell'INFN; gli utenti autorizzati al trattamento dei dati personali sono individuati come incaricati del trattamento ai sensi dell'art. 30 del D.Lgs. n. 196/03.

In ciascuna Sezione possono essere inoltre individuati uno o più Referenti per le questioni informatiche, che svolgono un ruolo di interfaccia tra i gruppi di utenti che rappresentano e il *Servizio Calcolo e Reti*.

7.2.3 Responsabilità

Di seguito è Rappresentato l'organigramma funzionale del *Servizio Calcolo e Reti* distinguendo tra le funzioni interne al servizio e quelle esterne; il Manuale del Sistema Gestionale Integrato – MSGI descrive il dettaglio dei compiti e delle responsabilità delle funzioni organizzative afferenti al *Servizio Calcolo e Reti* relativamente agli aspetti organizzativi del SGI ed in particolare alla sicurezza delle informazioni.



7.3 Scambio di informazioni

7.3.1 Obiettivi

Gestire gli scambi di informazioni con determinate strutture esterne, enti e/o organizzazioni pubbliche e private, senza compromettere l'integrità e la riservatezza delle informazioni e, nel contempo, garantire la sicurezza e la correttezza dell'operatività dei sistemi di elaborazione e di comunicazione.

7.3.2 Flussi di informazioni con altre organizzazioni

Il *Servizio Calcolo e Reti* garantisce lo scambio di informazioni con soggetti esterni regionali, nazionali ed internazionali; tali scambi di informazioni avvengono sulla base di norme di legge, accordi o protocolli d'intesa.

I flussi informativi con i soggetti esterni all'organizzazione sono caratterizzati dalla conformità alle regole concordate al fine di preservare l'integrità, la riservatezza, l'autenticità delle informazioni scambiate e la sicurezza dei sistemi di elaborazione nel rispetto della normativa, nazionale e comunitaria, vigente.

7.4 Gestione dei rischi

7.4.1 Obiettivi

Identificare e contrastare le possibili minacce alla sicurezza dei sistemi e delle informazioni del *Servizio Calcolo e Reti*, al fine di predisporre adeguate misure di prevenzione e protezione (vedi DVR e procedura di controllo del processo PCP01).

7.4.2 Interruzione dei servizi

La riduzione dei rischi connessi all'interruzione dei servizi è messa in pratica da una costante e continua azione di formazione ed informazione dei dipendenti, come previsto nei piani di formazione, circa le procedure di emergenza, il backup e la conservazione dei dati.

7.4.3 Accessi non autorizzati

La politica di sicurezza delle informazioni del *Servizio Calcolo e Reti* sono orientate alla protezione efficace da minacce provenienti da soggetti interni e/o esterni non autorizzati ad accedere ai sistemi di gestione delle informazioni, rendendo meno probabile l'intrusione e l'illecita sottrazione e utilizzazione illegale di informazioni.

7.4.4 Qualità dei dati

Viene effettuato il costante controllo degli aggiornamenti dei sistemi operativi e delle applicazioni software utilizzate, in modo da prevenire errori durante il loro utilizzo con conseguente aumento della qualità dei dati trattati e dell'efficienza operativa del personale.

7.4.5 Furti informatici

La riduzione delle possibilità di furti informatici è perseguita tramite il controllo degli accessi fisici ai locali ove sono svolte le attività del *Servizio Calcolo e Reti*, le cui procedure e misure di sicurezza sono descritte nei documenti del SGI in ottemperanza a quanto previsto dai documenti del progetto "Harmony – linee guida per la sicurezza informatica" emanati dalla CCR.

7.4.6 Software malevolo (virus, trojan, ecc.)

Uno dei grandi rischi per la sicurezza delle informazioni di una organizzazione è rappresentato dal "codice malevolo" (malware: Virus, trojan, ecc.). I rischi connessi al software malevolo sono affrontati con una politica di formazione ed informazione di personale ed utenti sui danni legati all'utilizzo di software diversi da quelli in dotazione. Contestualmente, il *Servizio Calcolo e Reti* è tutelato contro le minacce derivanti dal malware, dall'aggiornamento continuo dei programmi specifici per la sua rilevazione ed eliminazione e dall'attuazione di specifiche procedure.

7.5 Trattamento dei dati

Il *Servizio Calcolo e Reti* adotta la politica e le misure previste per il trattamento delle informazioni personali come descritto nello specifico documento emesso dalla CCR e facente parte del gruppo "Harmony – antiterrorismo" "Note per l'attuazione delle misure antiterrorismo" e come dettagliato nel documento PG08 – "Gestione degli incidenti di sicurezza delle informazioni".

I dipendenti del *Servizio Calcolo e Reti* sono tenuti ad attenersi a quanto disposto nel documento "Note per l'attuazione delle misure antiterrorismo" e, in quanto incaricati al trattamento dei dati personali sono stati informati e formati sulle modalità e sui comportamenti da tenere per il trattamento di dati personali.

Qualora i dipendenti di altre organizzazioni ovvero gli utenti che a vario titolo utilizzano, in nome e/o per conto, oppure sono autorizzati in base ad uno specifico titolo (convenzione, contratto, accordo, autorizzazione, ecc.), i sistemi di gestione delle informazioni e di rete del *Servizio Calcolo e Reti*, sono tenuti ad osservare le regole contenute nel documento "Note per l'attuazione delle misure antiterrorismo".

7.6 Continuità operativa

La responsabilità della Continuità Operativa dei servizi erogati dal *Servizio Calcolo e Reti* è di Resp. Servizio. Allo scopo è viene predisposto e mantenuto aggiornato un apposito piano di continuità operativa, inteso come indicazione delle attività organizzative e tecnologiche, finalizzate alla continuità dei servizi erogati dal *Servizio Calcolo e Reti*.

Nella predisposizione del piano di continuità operativa (vedi PG09), Resp. Servizio si avvale del supporto tecnico ed organizzativo, ciascuno per le proprie competenze, del personale del *Servizio Calcolo e Reti*.

7.6.1 Obiettivi

Garantire il ripristino di una situazione di normalità entro un tempo prestabilito, in relazione ai livelli di servizio attesi e rendere minimi gli impatti sui servizi erogati dall'organizzazione dovuti all'interruzione delle attività successive ad un guasto o disastro.

7.6.2 Requisiti per l'operatività

Il *Servizio Calcolo e Reti* ritiene che possono presentarsi degli eventi che possano portare all'interruzione dei servizi erogati e cerca, con le precauzioni contenute nel piano di continuità operativa di contenere l'impatto di tali eventi sulle proprie attività.

Il *Servizio Calcolo e Reti* riconosce che i sistemi di elaborazione delle informazioni sono elementi di criticità per la corretta erogazione dei servizi e una loro prolungata indisponibilità risulta dannosa per l'operatività dell'organizzazione e degli utenti, in particolare per l'erogazione dei servizi in qualità.

7.6.3 Elementi di pianificazione

Le metodologie che consentono di redigere, realizzare e mantenere il piano di continuità operativa sono diverse e fanno riferimento a standard organizzativi riconosciuti. Gli elementi comuni a tali standard sono:

- identificazione delle strutture di coordinamento della strategia di ripristino;
- valutazione dei risultati dell'Analisi dei Rischi per l'individuazione dei processi e dei servizi critici e delle priorità di intervento;
- predisposizione delle procedure da applicare in caso di attuazione del piano di continuità operativa; tali procedure sono definite nei documenti del SGSI;
- sviluppo, documentazione e verifica del piano di continuità operativa; nel *Servizio Calcolo e Reti* la verifica del BCP è annuale, e comunque conseguente a significativi cambiamenti degli elementi che lo compongono.

7.7 Inventario delle risorse

L'inventario delle risorse è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, e programmare gli investimenti in tecnologie dell'informazione.

7.7.1 Obiettivi

Identificare, classificare e registrare le risorse fisiche, hardware e software utilizzate dall'organizzazione, al fine di tracciare l'intero "ciclo di vita": acquisizione, assegnazione, aggiornamento, manutenzione, dismissione.

7.7.2 Inventario

Il *Servizio Calcolo e Reti* è dotato di un inventario informatizzato delle risorse che compongono la dotazione funzionale del servizio, la responsabilità della sua gestione è affidata a CO.

7.7.2.1 Inventario risorse fisiche

Le risorse fisiche sono identificate e classificate e per ciascuna di esse sono registrate le informazioni in esse contenute per la loro corretta gestione reperimento, aggiornamento e/o dismissione.

7.7.2.2 Inventario risorse hardware

Le risorse hardware sono classificate e per ciascuna di esse sono registrate le informazioni necessarie per la loro corretta gestione ed efficace manutenzione e/o aggiornamento.

7.7.2.3 Inventario risorse software

I programmi software sono classificati e per ciascuno di essi vengono registrate le informazioni per una corretta gestione, controllo ed efficace manutenzione e/o aggiornamento.

7.8 Sicurezza fisica ed ambientale

Costituisce la forma di tutela che attiene alla protezione dei sistemi di elaborazione delle informazioni e si manifesta con misure fisiche dirette a garantire i controlli contro accessi non autorizzati ai locali ove sono ubicati i sistemi di gestione delle informazioni.

Preserva l'integrità e la disponibilità dei sistemi di gestione ed elaborazione delle informazioni del *Servizio Calcolo e Reti* per mezzo di misure atte ad impedire l'accesso non autorizzato ai locali ove sono ubicati (vedi DVR e VMO).

7.8.1 Obiettivi

Minimizzare gli impatti delle minacce ai sistemi di gestione ed elaborazione delle informazioni dovuti a danni o intrusioni.

7.8.2 Sicurezza delle aree

Le aree che comprendono i locali ove risiedono le informazioni sono dotate punti di accesso controllati.

7.8.3 Sicurezza dei locali

I locali del *Servizio Calcolo e Reti* sono dotati di sistemi atti a garantire e mantenere la sicurezza e l'integrità delle attrezzature, apparecchiature e degli impianti, al fine di evitare guasti che possono causare interruzione fisica al funzionamento delle attività inerenti l'erogazione dei servizi.

7.8.4 Controllo degli accessi ai locali

Tutti i sistemi e apparecchiature di rete sono ubicati in aree sicure e con accesso controllato. In particolare, i locali ove risiedono i sistemi server e le apparecchiature di rete sono "aree ad accesso ristretto" e l'ammissione è consentita solo in presenza di personale interno dell'organizzazione autorizzato, come previsto dal documento emesso dalla CCR e facente parte del progetto "Harmony – antiterrorismo" "Note per l'attuazione delle misure antiterrorismo". L'accesso ai locali del *Servizio Calcolo e Reti* è regolamentato.

Chiunque, i dipendenti di altre organizzazioni ovvero gli utenti che a vario titolo utilizzano, in nome e/o per conto, oppure sono autorizzati in base ad uno specifico titolo (convenzione, contratto, accordo, autorizzazione, ecc.), i sistemi di gestione delle informazioni e di rete del *Servizio Calcolo e Reti*, sono tenuti ad osservare le regole di accesso ai locali descritte nel documento del progetto "Harmony – antiterrorismo" "Note per l'attuazione delle misure antiterrorismo".

Il personale del *Servizio Calcolo e Reti* al fine di garantire un adeguato grado di sicurezza, adotta la politica di scrivania pulita relativamente ai documenti ed ai supporti di memorizzazione gestiti, e di schermo pulito relativamente ai PC fissi ed ai PC portatili utilizzati.

7.9 Sicurezza logica

7.9.1 Obiettivi

Impedire accessi non autorizzati, tramite procedure di controllo, del personale del *Servizio Calcolo e Reti* e dei soggetti appartenenti a organizzazioni esterne che, in forza di titolo (delega, contratto, accordo, convenzione o autorizzazione), accedono alle applicazioni dell'organizzazione.

Proteggere le informazioni ed i sistemi di elaborazione e di comunicazione con misure tecnologiche ed organizzative atte a garantire il controllo degli accessi, la qualità delle informazioni, nonché la loro riservatezza ed integrità (vedi PCP01, DVR, VMO, PG08).

7.9.2 Accesso ai sistemi ed alle applicazioni

7.9.2.1 Regole di accesso

Il personale del *Servizio Calcolo e Reti* ed i soggetti esterni (utenti), devono accedere solo ai sistemi a cui sono stati autorizzati. Ogni abuso di accesso a sistemi diversi da quelli autorizzati, è perseguito ai sensi dell'articolo 615-ter del Codice Penale "Accesso abusivo ad un sistema informatico o telematico", così come modificato dalla Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

Qualora gli utenti dovessero accedere in modo incidentale a sistemi o ad applicazioni del *Servizio Calcolo e Reti* senza autorizzazione, sono tenuti a disconnettersi e segnalare l'anomalia al RSI del *Servizio Calcolo e Reti*.

7.9.2.2 Accesso alla rete

Il *Servizio Calcolo e Reti* provvede a dotare il proprio personale all'atto dell'insediamento, e i soggetti appartenenti a strutture esterne che, in forza di titolo (delega, contratto, accordo, convenzione o autorizzazione), della credenziale d'accesso alla rete. Le regole tecniche ed organizzative per la sicurezza della rete, dei dati e delle informazioni trattate con l'ausilio di strumenti elettronici, sono descritte negli specifici documenti emanati dalla CCR e facenti parte del "progetto Harmony – linee guida per la sicurezza informatica".

7.9.2.3 Accesso alle applicazioni

Il *Servizio Calcolo e Reti* abilita il proprio personale ed i soggetti appartenenti ad enti o organizzazioni con i quali è in essere un rapporto, ad essere autorizzati come utenti dei propri sistemi di elaborazione delle informazioni.

Il *Servizio Calcolo e Reti* adotta la profilazione degli utenti, sia interni che esterni, per la concessione della credenziale d'accesso alle applicazioni ed utilizza a tal fine una procedura formale, mantenendo documentazione cartacea ed elettronica, delle autorizzazioni concesse.

OP per le proprie competenze controlla almeno una volta all'anno, la validità di tutte le autorizzazioni attive per l'accesso alle applicazioni dell'organizzazione.

La revoca all'accesso ai sistemi di elaborazione delle informazioni del *Servizio Calcolo e Reti*, viene attuata qualora decadano le caratteristiche di abilitazione di un utente in conformità con le norme interne dell'INFN sui profili consentiti.

7.9.2.4 Caratteristiche e gestione delle password

Il *Servizio Calcolo e Reti* considera la password, conformemente alle norme di sicurezza informatica, come una "informazione confidenziale di autenticazione composta da una serie di caratteri e/o simboli", utilizzata per l'accesso ai sistemi di elaborazione dell'informazione.

Il *Servizio Calcolo e Reti* genera ed assegna password individuali e l'utente è responsabile della sua riservatezza.

Chiunque, è tenuto al rispetto delle regole definite all'interno del documento emanato dalla CCR e facente parte del gruppo Harmony - linee guida per la sicurezza informatica" denominato "Condizioni d'uso delle risorse informatiche".

La struttura delle password generate dai sistemi usati dal *Servizio Calcolo e Reti* presenta le seguenti caratteristiche informative e gestionali:

- obbligo di modifica al primo accesso;
- lunghezza minima di 8 caratteri;
- composizione con caratteri comprendenti almeno due lettere maiuscole, due minuscole e due numeri;
- validità massima minore di 180 gg;
- non ripetibilità delle tre password precedenti;
- disattivazione automatica dopo la decadenza dei requisiti stabiliti a livello nazionale e la tempistica definita attraverso i disciplinari..

7.9.3 Utilizzo e gestione del software

7.9.3.1 Gestione software su licenza

Il *Servizio Calcolo e Reti* utilizza software concesso da licenze ed autorizza i dipendenti e gli utenti amministratori, al loro uso.

Il *Servizio Calcolo e Reti* consente l'uso solo di software autorizzato installato sui sistemi all'atto della loro consegna e raccomanda agli utenti, in particolare per il software di "produttività individuale", una attenta analisi di quello installato sui propri sistemi. Software diverso da quello in dotazione standard e comunque conforme alla politica di sicurezza, deve essere richiesto da *Resp Servizio* a *Dir Sezione*, dopo aver riconosciuto la necessità funzionale.

Il *Servizio Calcolo e Reti* proibisce che sui sistemi dati in dotazione ai propri dipendenti o comunque i sistemi personali autorizzati all'accesso alla rete INFN sia installato software non autorizzato e considera illegale, ai sensi del D.Lgs. 9 aprile 2003 n. 68 "Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione", l'uso di software acquisito ed utilizzato senza regolare licenza d'uso.

7.9.3.2 Sviluppo di applicazioni software

All'interno del *Servizio Calcolo e Reti* non si effettua sviluppo di applicazioni software.

Eventuale sviluppo di applicazioni software, qualora ritenuto necessario e compatibile con la necessità di garantire la sicurezza delle informazioni, avviene in coerenza con la strategia dell'organizzazione ed orientato al supporto delle attività operative e direzionali, in una logica di ottimizzazione dell'efficienza, efficacia, della qualità e della sicurezza delle informazioni.

Il processo di realizzazione delle applicazioni informatiche nel *Servizio Calcolo e Reti*, siano esse nuove applicazioni o modifiche e/o manutenzioni di natura correttiva o evolutiva di quelle esistenti richiesti da variazioni normative, organizzative o da utenti, verrebbe svolto secondo i seguenti criteri:

- coerenza e uniformità con i documenti del SGSI relativi alla sicurezza delle applicazioni informatiche";
- pianificazione e controllo delle varie fasi: analisi, disegno, sviluppo, deployment, test nel rispetto delle relative procedure";
- conformità alle direttive comunitarie e nazionali sulla sicurezza delle informazioni ed allo standard UNI CEI/EN ISO/IEC 27001:2014.

7.10 Backup dei dati ed uso dei dispositivi di memorizzazione

Eventi dannosi o dovuti ad errori accidentali possono comportare perdita di dati conservati sul computer personale con ripercussioni anche gravi sull'attività lavorativa e sull'erogazione dei servizi (vedi PG09).

Al fine di evitare il rischio di perdita di dati importanti il *Servizio Calcolo e Reti* effettua il backup dei dati e delle informazioni gestite sui server.

il personale del *Servizio Calcolo e Reti* e gli utenti sono invitati a salvare periodicamente i dati residenti sul personal computer, nelle apposite cartelle di sistema o sui supporti messi a disposizione dall'organizzazione.

I supporti rimovibili che contengono o hanno contenuto dati personali, possono essere riutilizzati o ceduti solo se debitamente e previamente cancellati in modo tale che, in modo permanente, non sia tecnicamente possibile il recupero di tali dati, come indicato nei documenti del SGI e nei documenti emessi dalla CCR e facenti parte del gruppo Harmony – linee guida per la sicurezza informatica".

L'uso di supporti di memorizzazione rimovibili e di computer portatili, fuori dai locali del *Servizio Calcolo e Reti* è consentito al personale, solo per l'esecuzione di interventi da effettuare presso le postazioni degli utenti purchè sia garantita la classificazione nel registro degli Asset e ne venga garantita la sicurezza.

7.11 Sicurezza delle reti delle telecomunicazioni

Per garantire la sicurezza delle reti e delle comunicazioni occorre prevenire l'accesso alle reti e l'utilizzo illegale di informazioni, da parte di soggetti non autorizzati al fine di preservare la riservatezza dei dati e la disponibilità del servizio.

I documenti emessi dalla CCR e facenti parte del gruppo Harmony – linee guida per la sicurezza informatica". contengono le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato della posta elettronica e la protezione contro il software malevolo.

7.12 Gestione degli incidenti informatici

Un incidente, nell'ambito della sicurezza dell'informazione, è un evento sospetto o una vulnerabilità tale da violare l'integrità, la riservatezza e/o la disponibilità delle applicazioni, dei dati e/o dei sistemi di elaborazione delle informazioni (vedi PG08).

Tutti, personale del *Servizio Calcolo e Reti* ed utenti, devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nei documenti emessi dalla CCR e contenuti nel gruppo Harmony – linee guida per la sicurezza informatica".

Chiunque individua o abbiano il sospetto di un possibile incidente riguardante la sicurezza delle informazioni, deve segnalarlo ad RSI.