Disciplinare per l'uso delle risorse informatiche nell'INFN

24 Gennaio 2020

1. PRINCIPI GENERALI

L'Istituto Nazionale di Fisica Nucleare (INFN) è un ente pubblico nazionale di ricerca disciplinato dalle norme contenute nel proprio Statuto.

L'INFN considera le risorse di calcolo ed i servizi di rete, nonché i dati e le informazioni da questi trattati, parte integrante del proprio patrimonio e funzionali al raggiungimento delle proprie finalità istituzionali di ricerca scientifica e tecnologica.

Con il presente Disciplinare l'INFN intende salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati.

L'INFN, aderendo all'associazione Consortium GARR - Rete italiana dell'Università e della Ricerca - e utilizzandone i relativi servizi e strumenti, intende assicurare con il presente Disciplinare la conformità delle proprie norme con quelle dettate dal Consortium GARR.

Nell'INFN il trattamento dei dati raccolti in relazione all'uso delle risorse di calcolo e dei servizi di rete avviene solo per finalità determinate, esplicite e legittime, nel rispetto dei principi di necessità, pertinenza, correttezza e non eccedenza secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. I sistemi informativi e i programmi informatici sono pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi.

Tutti coloro ai quali è consentito l'accesso alle risorse di calcolo e ai servizi di rete sono tenuti al rispetto delle norme di seguito esposte, che definiscono ed integrano i doveri minimi di condotta previsti nel Codice di Comportamento dell'INFN, oltre comunque a un comportamento ispirato ai principi di correttezza e diligenza.

2. AMBITO DI APPLICAZIONE

Il presente Disciplinare si applica a tutti coloro cui sia stato consentito l'accesso alle risorse di calcolo ed ai servizi di rete dell'INFN.

3. DEFINIZIONI

Per **risorse di calcolo** e **servizi di rete** si intendono:

- elaboratori e analoghi dispositivi elettronici, stampanti e altre periferiche (ad es. *scanner* e sistemi di storage) di proprietà dell'Ente o comunque connesse alla rete dell'Ente;
- apparati e infrastrutture di rete di proprietà dell'Ente o comunque connessi alla rete dell'Ente;
- il servizio di connettività alle reti locali e geografiche con esclusione della mera connettività geografica garantita tramite accordi tra Istituzioni e Federazioni (ad es. Eduroam);
- istanze virtuali di calcolatori o apparati di rete;
- software e dati acquistati, prodotti o pubblicati dall'Ente.

Nell'ambito del presente Disciplinare le risorse di calcolo ed i servizi di rete possono essere collettivamente definite **risorse informatiche**.

I soggetti che operano con le risorse informatiche dell'INFN si distinguono in:

- **Utente**: ogni soggetto che abbia accesso alle risorse di calcolo e ai servizi di rete dell'INFN, in relazione alle funzioni ed attività che svolge nell'ambito dell'Istituto;
- **Referente di gruppo di utenti**: un soggetto che coordina gli utenti e l'uso delle risorse locali di uno o più gruppi, esperimenti o servizi, in conformità alle indicazioni del Servizio di Calcolo e Reti;
- **Amministratore di sistema**: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza;
- **Servizio di Calcolo e Reti**: il servizio cui compete la gestione delle risorse di calcolo centrali, i collegamenti in rete all'interno ed all'esterno di ciascuna Struttura, nonché la cura, installazione e 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 Struttura;
- **Direttore di Struttura**: il soggetto al quale, nel rispetto degli indirizzi approvati dal Consiglio Direttivo, compete la responsabilità di assicurare il funzionamento scientifico, organizzativo ed amministrativo di ciascuna Struttura come individuata nelle norme dello Statuto INFN.

4. ACCESSO ALLE RISORSE INFORMATICHE

L'accesso alle risorse di calcolo e ai servizi di rete dell'INFN è consentito, previa identificazione, ai dipendenti e agli associati, nonché a collaboratori, ospiti, dottorandi, specializzandi, assegnisti, borsisti, laureandi o altri autorizzati secondo le norme del presente Disciplinare.

L'autorizzazione all'accesso è rilasciata dal Direttore di Struttura o da un suo delegato per un periodo temporale limitato alla durata del rapporto sulla base del quale è consentita l'attività all'interno dell'INFN.

L'accesso è personale, non può essere condiviso o ceduto e il relativo utilizzo è consentito a ciascun utente soltanto in conformità alle norme del presente Disciplinare.

5. DISPOSIZIONI GENERALI PER L'USO DELLE RISORSE INFORMATICHE

Le risorse informatiche, in quanto essenziali per l'INFN, sono rese disponibili per il conseguimento delle finalità istituzionali dell'Ente.

Gli utenti sono tenuti a servirsi delle risorse informatiche dell'Ente prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

1. attività contrarie alla legge nazionale, comunitaria e internazionale o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
2. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (spamming) o l'uso delle proprie risorse da parte di terzi per tali attività;
3. attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza e/o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, la religione, le opinioni politiche o la condizione personale o sociale;
4. attività comunque non conformi ai fini istituzionali dell'Ente.

L'utilizzo delle risorse informatiche per finalità personali è tollerato purché non violi le leggi applicabili e sia compatibile con le norme del presente Disciplinare e di tutte le indicazioni stabilite dall'INFN.

6. DISPOSIZIONI SPECIFICHE PER L'USO DELLE RISORSE INFORMATICHE

Al fine di garantire la sicurezza delle risorse di calcolo e dei servizi di rete è vietato:

1. connettere risorse di calcolo alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del Servizio di Calcolo e Reti;
2. cablare, collegare o modificare apparati di rete senza l'autorizzazione del Servizio di Calcolo e Reti;
3. utilizzare indirizzi di rete e nomi non espressamente assegnati;
4. installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del Servizio di Calcolo e Reti;

5. fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
6. divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento a quelle che consentono accesso da remoto;
7. accedere senza autorizzazione ai locali del Servizio di Calcolo e Reti, nonché ai locali ed alle aree riservate alle apparecchiature di rete;
8. intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire ai soggetti autorizzati l'accesso alle risorse, ottenere risorse superiori a quelle autorizzate o accedere alle risorse di calcolo violandone le misure di sicurezza.

Gli **Utenti** inoltre:

1. sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio di Calcolo e Reti in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'INFN in materia e pubblicate nelle pagine web del DPO INFN e dei Servizi Calcolo e Reti delle Strutture.
2. nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del Servizio di Calcolo e Reti, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;
3. sono responsabili dei dati e del software che installano sui computer loro affidati: procedono ad una loro attenta valutazione preliminare e non installano software privi delle regolari licenze;
4. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso;
5. valutano attentamente l'affidabilità dei servizi esterni eventualmente utilizzati, ivi inclusi quelli di tipo *cloud*, in termini di sicurezza, conservazione e confidenzialità dei dati;
6. sono tenuti a seguire le indicazioni del Servizio di Calcolo e Reti per il salvataggio periodico dei dati e programmi utilizzati;
7. sono tenuti a proteggere il proprio account mediante password che rispettino le norme di sicurezza indicate dall'Ente e dal Servizio Calcolo e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema;
8. non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
9. sono tenuti a segnalare immediatamente al proprio Referente e al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza;
10. per i sistemi operativi che lo prevedono, devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili utilizzati;
11. non devono mantenere connessioni remote inutilizzate né abbandonare la postazione di lavoro con connessioni aperte non protette.
12. sono tenuti, al termine del rapporto di lavoro/collaborazione con l'INFN a trasferire al proprio responsabile, o al Direttore di Struttura o al soggetto da questo delegato, i file di contenuto inerente l'attività di servizio/collaborazione e a cancellare in via definitiva eventuali altri file. Entro il termine di due mesi dalla cessazione del

rapporto, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente secondo le modalità indicate nel provvedimento del Garante per la tutela dei dati personali del 13 ottobre 2008. In caso di impossibilità o impedimento dell'Utente, ovvero laddove lo stesso, prima della cessazione del rapporto, non abbia reso disponibili i file attinenti l'attività di servizio/collaborazione e non abbia delegato un collega a inoltrarli, il Direttore, o un suo delegato, può accedere alle risorse assegnategli per il periodo necessario a recuperare i dati di interesse. In caso di grave improvvisa indisponibilità o decesso dell'Utente, il Direttore, su richiesta, potrà rendere disponibile agli aventi diritto i file con contenuti personali.

Gli **Utenti** che hanno privilegi di amministratore sui loro sistemi (p.e. laptop) sono tenuti a prendere visione dei relativi documenti con le Norme d'uso, in attuazione della Circolare AgID 18/04/2017 n. 2/2017, e a seguirne scrupolosamente le indicazioni.

7. INDIVIDUAZIONE E COMPITI DEL REFERENTE DI GRUPPO DI UTENTI

Il Referente del gruppo di utenti è individuato dal Direttore della Struttura cui afferisce in ragione delle funzioni assegnate. Il Referente può essere altresì individuato dalla collaborazione scientifica cui appartiene. La designazione è comunicata al Servizio di Calcolo e Reti competente.

Il **Referente**:

1. divulga, nell'ambito del proprio gruppo, le indicazioni del Servizio di Calcolo e Reti relative alla sicurezza delle risorse ed al corretto uso delle stesse;
2. in caso di necessità, fornisce al Servizio di Calcolo e Reti informazioni o accesso alle risorse di calcolo del proprio gruppo.

8. INDIVIDUAZIONE E COMPITI DEGLI AMMINISTRATORI DI SISTEMA

Gli **Amministratori di Sistema** sono designati dal Direttore della Struttura di afferenza con apposito atto.

Nel caso in cui l'attività dell'Amministratore di Sistema riguardi risorse informatiche collocate presso più Strutture, l'atto di designazione è comunicato al Direttore e al Servizio di Calcolo e Reti di ciascuna Struttura.

Gli **Amministratori di sistema**, oltre all'osservanza di tutte le disposizioni precedenti, sono tenuti a:

1. mantenere i sistemi al livello di sicurezza appropriato al loro uso;
2. verificare con regolarità l'integrità dei sistemi;
3. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
4. segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e

violazioni della sicurezza e partecipare alla loro gestione;

5. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;
6. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;
7. in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
8. seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

9. COMPITI DEL SERVIZIO CALCOLO E RETI

Il **Servizio Calcolo e Reti**, al fine di mantenere il più elevato livello di sicurezza all'interno delle reti locali, in relazione all'evoluzione tecnologica del settore:

1. controlla che gli accessi remoti alle risorse locali avvengano esclusivamente mediante l'uso di protocolli che prevedano l'autenticazione e la cifratura dei dati trasmessi;
2. limita l'uso interno di servizi e programmi che trasmettono in chiaro le password;
3. sulle macchine gestite, provvede a disattivare i servizi non essenziali ed a limitare il numero degli utenti privilegiati a quello strettamente necessario per le attività di coordinamento, controllo e monitoraggio della rete e dei servizi ad essa afferenti;
4. effettua la revisione, almeno annuale, degli account;
5. effettua il monitoraggio della rete e dei sistemi gestiti, incluse le risorse utilizzate per l'erogazione di servizi di tipo *cloud*, al fine di garantirne la funzionalità e la sicurezza;
6. realizza i sistemi di filtraggio e logging sugli apparati perimetrali della rete;
7. fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti.

10. DISPOSIZIONI PER L'USO DEI SERVIZI ESTERNI

Il trattamento dei dati personali di qualunque tipo o di particolare rilevanza per l'Ente può essere effettuato mediante l'uso di servizi esterni, anche di tipo *cloud*, soltanto ove l'INFN abbia preventivamente verificato i rischi e i benefici connessi ai servizi offerti, i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati oltre ai profili di responsabilità nel trattamento.

11. TRATTAMENTO DEI DATI ACQUISITI IN RELAZIONE ALL'USO DELLE RISORSE DI CALCOLO E ALL'ACCESSO AI SERVIZI DI RETE

L'INFN, nel rispetto dei principi di libertà e dignità, non consente l'installazione di strumentazioni hardware e software mirate al controllo degli utenti e vieta il trattamento effettuato mediante apparecchiature preordinate al controllo a distanza quali:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio di posta elettronica;

b) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;

c) la lettura e registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi;

d) l'analisi occulta di computer portatili affidati in uso.

Con riferimento all'accesso alla rete, il Servizio Calcolo e Reti, per le finalità indicate al punto successivo raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente; non registra il contenuto delle connessioni, può raccogliere tuttavia alcune informazioni relative alle transazioni eseguite quali: indirizzi dei nodi, ora di inizio e fine transazione e quantità dei dati trasferiti.

I dati di cui al paragrafo precedente sono conservati per un periodo non superiore a un anno e sono utilizzabili dal personale del Servizio di Calcolo e Reti competente solamente con fini di controllo della sicurezza e per l'ottimizzazione dei sistemi.

Le Strutture in cui sono installati proxy server o altri sistemi di controllo delle sessioni possono conservare i file di log contenenti informazioni relative alle pagine web, interne od esterne, accedute dai nodi locali. Tali informazioni, conservate per un periodo non superiore a sette giorni a cura del Servizio di Calcolo e Reti, sono esaminate o elaborate soltanto ove si ravvisi la necessità di garantire la sicurezza o il buon funzionamento del sistema.

12. RACCOLTA DATI IN RELAZIONE AL SERVIZIO DI POSTA ELETTRONICA

Il Servizio di Calcolo e Reti per esigenze organizzative connesse al funzionamento, sicurezza e salvaguardia del servizio di posta elettronica registra data, ora, indirizzi del mittente e del destinatario dei messaggi di posta, nonché il risultato delle analisi dei software antivirus ed antispam.

I dati registrati, utilizzati anche per elaborazioni statistiche, sono conservati per un periodo non superiore a un anno e sono accessibili dal solo personale, appositamente incaricato, del Servizio di Calcolo e Reti di competenza.

Per le medesime finalità le Strutture che effettuano copie di salvataggio dei messaggi di posta elettronica conservano tali copie per un periodo non superiore a un anno a cura del Servizio di Calcolo e Reti di competenza.

Ciascuna Struttura, ove compatibile con la propria organizzazione, può rendere disponibili indirizzi di posta elettronica condivisi attraverso l'uso di liste di distribuzione di e-mail, nonché messaggi di risposta automatica, in caso di assenza programmata dei titolari.

La casella di posta elettronica è disattivata entro i due mesi successivi alla scadenza del

termine nel quale l'utente è stato autorizzato all'accesso. Entro tale periodo l'utente ha il dovere di trasferire al Direttore o a un suo delegato le comunicazioni di servizio d'interesse e di trasmettergli quelle nel frattempo intervenute. Il contenuto della casella è comunque cancellato entro un anno dalla scadenza del termine di autorizzazione all'accesso. I periodi indicati nel presente capoverso possono essere prolungati dal Direttore ove ne ravvisi specifica esigenza.

In caso di impossibilità o impedimento del titolare della casella di posta elettronica, il Direttore o un suo delegato può avere accesso alla casella per un periodo non superiore a un mese dalla data di conoscenza della situazione che ha determinato l'impossibilità o l'impedimento.

13. ULTERIORI MISURE PER LA TUTELA DEI SISTEMI INFORMATIVI

Al fine di assicurare la funzionalità, disponibilità, ottimizzazione, sicurezza ed integrità dei sistemi informativi e prevenire utilizzazioni indebite, l'INFN adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine il Servizio di Calcolo e Reti può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.

Nel caso in cui, nonostante l'adozione di accorgimenti tecnici preventivi, si verifichino eventi dannosi o rilevino comportamenti anomali o non consentiti, il Servizio di Calcolo e Reti esegue, previa informazione agli interessati e salvo i casi di necessità ed urgenza, ulteriori accertamenti e adotta le misure necessarie ad interrompere le condotte dannose o non consentite.

Nei casi di reiterazione di comportamenti vietati e già segnalati o di particolare gravità, il Responsabile del Servizio di Calcolo e Reti adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al Direttore di Struttura, che dispone gli ulteriori provvedimenti ai sensi del punto seguente.

I Direttori di Struttura, in relazione alle funzioni loro assegnate circa il trattamento dei dati personali, adottano ogni opportuna misura affinché i soggetti preposti al trattamento dei dati relativi all'uso di internet e della posta elettronica svolgano soltanto le operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, neppure di propria iniziativa.

14. VIOLAZIONE DELLE NORME

Ogni condotta posta in essere in violazione del presente Disciplinare potrà determinare la sospensione dell'accesso alle risorse di rete, salvo eventuali azioni disciplinari, civili o penali.

La violazione delle disposizioni del presente Disciplinare che cagioni a terzi un danno risarcito dall'INFN potrà determinare, nei confronti del responsabile, l'esercizio del diritto di rivalsa nelle forme e nei limiti stabiliti dalla legge.

15. INFORMATIVA

Il presente Disciplinare costituisce informativa ai sensi dell'art. 4, c. 3, della legge 20 maggio 1970 n.300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse di calcolo e dei servizi di rete.

L'INFN assicura al presente Disciplinare e ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti mediante pubblicazione nella pagina web di ciascuna Struttura, nonché consegnandolo a ciascuno in modalità elettroniche o cartacee, idonee comunque a dimostrare l'avvenuta consegna.

Il presente Disciplinare abroga e sostituisce integralmente tutti i precedenti regolamenti adottati in materia.

16. CLAUSOLA DI REVISIONE

Il presente Disciplinare è aggiornato periodicamente in relazione all'evoluzione della tecnologia e della normativa di settore.