Disciplinare
per l'uso delle risorse informatiche dell'INFN

Ottobre 2025

Rev. 26/10/2025

1. Principi generali

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, raccolti, prodotti o comunque trattati.

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

Nell'INFN il trattamento dei dati raccolti attraverso l'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 (**GDPR** nel seguito).

L'INFN, per il raggiungimento delle proprie finalità istituzionali, implementa, utilizza e gestisce sistemi di intelligenza artificiale nel rispetto di quanto previsto dalla normativa europea e nazionale tutelando i valori, le libertà, i diritti e l'autonomia dell'individuo che considera parte attiva e fondamentale del progresso umano e scientifico.

2. Ambito di applicazione

Il presente Disciplinare si applica a tutti coloro cui sia stato consentito l'accesso alle risorse informatiche dell'INFN.

Le norme di seguito esposte integrano i doveri minimi di condotta previsti nel Codice di Comportamento dell'INFN[1].

[1] https://l.infn.it/codicecomportamento

3. Definizioni

Per **risorse informatiche** si intendono:

- elaboratori e analoghi dispositivi elettronici, stampanti e altre periferiche 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;
- basi di dati e sistemi per la loro gestione;
- infrastrutture e servizi erogati dalle Strutture dell'Ente e centralmente attraverso la Direzione Sistemi Informativi e i Servizi Nazionali della CCR;
- infrastrutture e servizi erogati o gestiti dall'Ente su cloud INFN (DataCloud) o su cloud esterne, anche commerciali;
- software e dati acquistati, prodotti o pubblicati dall'Ente;

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

- **utente**: ogni soggetto che abbia accesso alle risorse informatiche dell'Ente, in relazione alle funzioni ed attività che svolge nell'ambito dell'Istituto;
- **utente privilegiato**: ogni soggetto che abbia credenziali di amministratore della risorsa individuale assegnata, senza essere nominato amministratore di sistema;
- **amministratore di sistema**: figura professionale, dotata di credenziali privilegiate, dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, i servizi web, le reti locali e gli apparati di sicurezza;
- **team responsabile delle risorse informatiche**: il gruppo cui compete la gestione e la sicurezza delle risorse informatiche, i collegamenti in rete all'interno ed all'esterno di ciascuna Struttura o diverso contesto, nonché la cura, l'installazione, lo sviluppo e l'assistenza; si intendono tali i Servizi di Calcolo presso le Strutture, la Direzione Sistemi Informativi (DSI), il gruppo di gestione di INFN DataCloud e ogni altro team che venga qualificato come tale da un organo dell'Istituto o dal Direttore di riferimento;
- **direttore di riferimento:** il direttore della Struttura cui afferiscono le risorse informatiche e il team responsabile delle stesse; nel caso di infrastrutture distribuite, la figura esplicitamente incaricata da un organo dell'Istituto.

4. Accesso alle risorse informatiche

L'accesso alle risorse informatiche dell'INFN è consentito, previa identificazione, ai dipendenti e agli associati, a collaboratori, ospiti, dottorandi, specializzandi, assegnisti, borsisti, laureandi, anche afferenti a enti, aziende o organizzazioni partner di INFN all'interno di progetti, collaborazioni, contratti, o altri autorizzati secondo le norme del presente Disciplinare.

L'identificazione deve avvenire tramite verifica di un documento di identità in corso di validità o tramite procedure o strumenti equivalenti.

L'accesso alle risorse è inoltre subordinato alla accettazione del presente disciplinare, delle regole

d'uso accessorie[2], eventuali ulteriori AUP e ToU specifici del servizio nonché al superamento di un corso di sicurezza informatica di livello adeguato alla criticità delle risorse[3].

L'accesso alle risorse è verificato tramite credenziali di autenticazione individuali.

Nel caso in cui l'accesso sia consentito a soggetti esterni all'INFN, l'identificazione, la verifica della competenza in sicurezza informatica e l'autenticazione possono essere demandati all'Organizzazione di afferenza, previo accordo inserito nel documento di collaborazione che garantisca il soddisfacimento dei requisiti sopra elencati.

L'autorizzazione all'accesso, per la durata del rapporto in base al quale è consentito l'utilizzo delle risorse informatiche dell'INFN, è rilasciata dal direttore di riferimento, o da un suo delegato.

L'accesso è personale e non può essere condiviso o ceduto.

5. Disposizioni generali

Le risorse informatiche sono asset essenziali per l'INFN, e 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 perché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

1. attività contrarie alla legge nazionale, comunitaria e internazionale;
2. attività proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
3. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto o l'uso delle proprie risorse da parte di terzi per tali attività;
4. attività idonee a danneggiare, distruggere o compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza 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, l'etnia, la religione, le opinioni politiche, la condizione personale o sociale;
5. attività che possano nuocere alla reputazione dell'Ente;
6. 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, non interferisca con il corretto funzionamento delle infrastrutture, sia compatibile con le norme del presente Disciplinare e delle regole d'uso accessorie[2] e sia limitato in durata e frequenza.

6. Disposizioni specifiche per l'uso delle risorse informatiche

Per motivi di sicurezza informatica è vietato:

1. connettere risorse di calcolo alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del team responsabile delle risorse informatiche;
2. collegare apparati di rete o modificarne la configurazione senza l'autorizzazione del team responsabile delle risorse informatiche;
3. utilizzare indirizzi e nomi di rete senza l'autorizzazione del team responsabile delle risorse

[2] https://security.infn.it/computing-rules

[3] https://security.infn.it/computing-rules/formazione-sicurezza-informatica

informatiche;

4. installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del team responsabile delle risorse informatiche;
5. fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
6. divulgare informazioni classificate come riservate sulla struttura e configurazione delle risorse informatiche, in particolare quelle che consentono accesso da remoto;
7. accedere senza autorizzazione ai locali dedicati ad ospitare risorse di calcolo, nonché alle aree riservate alle apparecchiature di rete;
8. intraprendere qualsiasi azione diretta a degradare le risorse del sistema, impedirne l'accesso ai soggetti autorizzati, ottenere risorse superiori a quelle autorizzate o accedere alle risorse violandone le misure di sicurezza.

6.1 Utenti

Gli **utenti**, in aggiunta alle disposizioni già indicate:

1. sono tenuti ad agire nel rispetto delle indicazioni in materia di sicurezza informatica fornite dal Nucleo Cybersecurity dell'INFN (NUCS), dal team responsabile delle risorse informatiche nonché delle norme dettate dall'INFN per il trattamento dei dati personali reperibili nelle pagine web del DPO[4].
2. sono responsabili dei dati e del software che installano sulle risorse informatiche loro affidate, procedono a una loro attenta valutazione preliminare e non installano per nessuna ragione software privi delle regolari licenze;
3. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati o memorizzati nei sistemi cui hanno accesso;
4. sono tenuti a proteggere il proprio account mediante password che rispettino le relative norme di sicurezza[5];
5. non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
6. sono tenuti a seguire le indicazioni del team responsabile delle risorse informatiche per il salvataggio periodico dei dati e programmi;
7. non devono aggirare le misure di isolamento e di sicurezza delle risorse assegnate;
8. sono tenuti a segnalare immediatamente al team responsabile delle risorse informatiche incidenti, sospetti abusi e violazioni della sicurezza;
9. devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili prima del loro utilizzo;
10. non devono mantenere connessioni remote inutilizzate né abbandonare la postazione di lavoro con connessioni aperte non protette;
11. se utilizzano dispositivi mobili sono tenuti a rispettare le indicazioni del paragrafo **Dispositivi mobili**;
12. sono tenuti, al termine del rapporto con l'INFN a trasferire al proprio responsabile, o al direttore di riferimento o al soggetto da questo delegato, i dati relativi all'attività lavorativa e a cancellare gli altri;
13. devono rispettare ogni altra indicazione in materia che dovesse essere fornita dall'Ente.

[4] https://dpo.infn.it

[5] https://security.infn.it/computing-rules/password-policy

6.2 Utenti privilegiati

Gli **utenti privilegiati**, oltre a soddisfare le disposizioni precedenti**:**

1. devono prendere visione dei documenti con le norme tecniche d'uso per i dispositivi informatici individuali[6] e seguirne le indicazioni;
2. non possono dare accesso alle loro risorse ad altri utenti;
3. non devono interferire con il sistema di raccolta dei log;
4. devono utilizzare, sui sistemi che li supportano, programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili prima del loro utilizzo;
5. devono rispettare ogni altra indicazione che dovesse essere fornita dall'Istituto in materia.

6.3 Amministratori di sistema

Gli amministratori di sistema sono nominati individualmente dal direttore di riferimento o da figura da esso delegata. In caso di utenti esterni, la nomina può essere a cura dell'Organizzazione di afferenza, secondo le modalità indicate nell'accordo di collaborazione.

Gli **amministratori di sistema**, oltre a soddisfare 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. dare accesso alle risorse assegnate solo dopo aver verificato che l'utente rispetti le condizioni indicate nel paragrafo **Accesso alle risorse informatiche**;
5. conservare l'associazione tra gli account e le identità degli utenti;
6. non condividere l'accesso privilegiato alle risorse assegnate;
7. segnalare immediatamente al team responsabile delle risorse informatiche incidenti, sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione;
8. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;
9. non visionare dati personali o corrispondenza, salvo per necessità tecniche, e in generale considerare sempre tali informazioni strettamente riservate;
10. in caso di interventi di manutenzione da parte di supporto esterno, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
11. seguire attività formative in materie tecnico-gestionali, di sicurezza delle reti, dei sistemi o dei servizi amministrati, e di protezione dei dati personali;
12. rispettare ogni altra indicazione in materia che dovesse essere fornita dall'Istituto.

6.4 Team responsabile delle risorse informatiche

Il **team responsabile delle risorse informatiche**:

1. ha in carico la gestione e la sicurezza delle risorse informatiche di propria competenza;
2. è tenuto a rispettare le indicazioni in materia di sicurezza informatica fornite dal Nucleo Cybersecurity dell'INFN (NUCS)

[6] https://security.infn.it/computing-rules

3. è tenuto a dare accesso alle risorse assegnate solo dopo aver verificato che l'utente rispetti le condizioni indicate nel paragrafo **Accesso alle risorse informatiche**;
4. 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;
5. disattiva i servizi non essenziali sulle macchine gestite e limita 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;
6. effettua la revisione, almeno annuale, degli account;
7. effettua il monitoraggio della rete e dei sistemi gestiti, incluse le risorse utilizzate per l'erogazione di servizi di tipo cloud, per garantirne la funzionalità e la sicurezza;
8. realizza i sistemi di filtraggio e di log sugli apparati perimetrali della rete;
9. segnala immediatamente al NUCS gli incidenti di sicurezza;
10. fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti;
11. rispetta ogni altra indicazione in materia che dovesse essere fornita dall'Istituto.

7. Sistemi di intelligenza artificiale

L'impiego dei Sistemi di Intelligenza Artificiale deve assicurare il rispetto delle leggi vigenti e dei principi di economicità, efficacia, efficienza, imparzialità, pubblicità, trasparenza, correttezza, responsabilità, sicurezza, sostenibilità ambientale, non discriminazione, tutela della riservatezza dei dati personali e della proprietà intellettuale.

A tale scopo l'utilizzo della IA nell'INFN è consentito nel rispetto delle norme e di eventuali disciplinari o linee guida sviluppati appositamente.

Al fine di garantire il rispetto della riservatezza dei dati, anche in relazione al GDPR, l'utilizzo di strumenti di Intelligenza Artificiale esterni è equiparato all'utilizzo di servizi esterni in generale, e disciplinato nel paragrafo **Disposizioni per l'uso di servizi esterni.**

8. Disposizioni per l'uso dei servizi esterni

Il trattamento dei dati personali di qualunque tipo, o dati di particolare rilevanza per l'Ente, può essere effettuato mediante l'uso di servizi informatici forniti da soggetti esterni soltanto ove l'INFN, mediante il DPO, il team responsabile delle risorse informatiche o altre figure competenti in materia, 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 nonché i profili di responsabilità nel trattamento e definito la qualificazione dei rapporti in relazione alla disciplina del GDPR.

Nel caso di servizi cloud destinati alle attività gestionali dell'Istituto, questi devono essere qualificati per l'uso da parte della Pubblica Amministrazione.

L'elenco dei servizi esterni approvati in funzione della tipologia di utilizzo[7] è mantenuto aggiornato dalla Commissione Calcolo e Reti.

[7] https://security.infn.it/computing-rules/servizi-esterni

9. Dati acquisiti in relazione all'uso delle risorse informatiche

L'INFN 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.

L'INFN vieta il trattamento dei dati personali acquisiti per qualsiasi motivo allo scopo di controllo e profilazione delle attività degli utenti, con le eccezioni e nei limiti di seguito indicati.

9.1 Dati utente

l'INFN mette a disposizione degli utenti sistemi per l'archiviazione dei propri dati che supportano strumenti per la protezione in lettura e scrittura. È responsabilità dell'utente adottare le necessarie configurazioni per proteggerli adeguatamente.

Il team responsabile delle risorse informatiche può accedere a tali dati in caso di malfunzionamenti, per salvare copie di sicurezza, o quando esplicitamente richiesto dall'utente stesso.

Tali informazioni possono contenere dati personali.

9.2 Backup e restore

Per garantire la resilienza dei dati di sistemi, servizi e utenti, il team responsabile delle risorse informatiche ne acquisisce e salva copia quotidiana e/o settimanale.

Questi dati possono contenere dati personali.

Questo trattamento viene effettuato unicamente allo scopo di ripristinare la disponibilità dei dati stessi in caso di necessità.

I backup vengono conservati per un periodo non superiore a 12 mesi, al termine del quale vengono cancellati definitivamente dai sistemi di storage.

9.3 Dati di log

Per garantire la funzionalità operativa dei sistemi e dei servizi informatici il team responsabile delle risorse informatiche acquisisce e salva dati di log delle applicazioni e delle connessioni di rete.

Tali dati possono contenere dati personali.

I log vengono salvati su sistemi accessibili al solo personale del team, e possono essere analizzati allo scopo di affrontare e risolvere eventuali malfunzionamenti o eventi di sicurezza informatica.

I log vengono conservati per un periodo di tempo non superiore a 6 mesi, al termine del quale vengono cancellati definitivamente.

9.4 Dati per la sicurezza informatica

Al fine di contrastare tentativi di accesso non autorizzato e supportare al meglio la protezione e la sicurezza di dati e servizi, il NUCS ed il team responsabile delle risorse informatiche possono acquisire in modo automatizzato informazioni relative alle configurazioni dei dispositivi connessi alle reti INFN, alle connessioni di rete ed alle attività degli utenti

Le informazioni raccolte, che possono contenere dati personali, vengono salvate su sistemi dedicati alla cybersicurezza, su risorse interne o su servizi cloud esterni. Se su cloud esterna, tali risorse ottemperano ai requisiti specificati nel paragrafo "**Disposizioni per l'uso dei servizi esterni**".

I dati relativi sono in esclusiva disponibilità del NUCS e del team responsabile delle risorse

informatiche e vengono trattati al solo scopo di individuare e gestire o prevenire incidenti di sicurezza informatica.

I dati vengono trattati da strumenti automatizzati. In caso di potenziale anomalia, i dati pertinenti vengono analizzati manualmente; in questo caso gli utenti coinvolti vengono informati su quanto di loro competenza ed eventualmente invitati a fornire ulteriori informazioni riguardo l'incidente.

Gli utenti devono collaborare con il personale del NUCS o del team e fornire tutti gli elementi a propria conoscenza.

I dati raccolti per le attività di sicurezza informatica vengono conservati per un periodo di tempo non superiore a 6 mesi, al termine del quale vengono cancellati definitivamente.

In caso di incidente di impatto rilevante i dati relativi possono venire conservati in modalità criptata per periodi più lunghi, per consentire l'adempimento degli obblighi conseguenti e favorire le verifiche e ispezioni da parte delle Autorità competenti

9.5 Posta elettronica

L'inoltro automatico dell'intera casella di posta elettronica INFN verso domini non INFN, in particolare verso domini commerciali non è consentito.

I metadati relativi alla posta elettronica (log) vengono trattati come descritto nel capitolo "**Dati di log**", ma per un periodo di tempo non superiore a 21 giorni.

La casella di posta elettronica è disattivata alla scadenza del termine di autorizzazione all'accesso alle risorse INFN, attivando se possibile un sistema che informi di indirizzi alternativi riferiti alla sua attività professionale.

Il contenuto della casella è cancellato entro 12 mesi dalla scadenza del termine di autorizzazione all'accesso. Questo periodo può essere prolungato dal Direttore di riferimento per motivate ragioni connesse alle esigenze di servizio.

9.6 Dati particolari

Ai sensi del GDPR, i dati personali che rivelino l'origine etnica, le opinioni politiche, le convinzioni religiose, filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute, alla vita o all'orientamento sessuale, a condanne penali e reati richiedono un livello più elevato di sicurezza e di tutela.

Il trattamento di dati personali e di dati particolari viene effettuato solo da personale esplicitamente incaricato e adeguatamente formato.

La trasmissione di dati particolari deve comunque essere sempre effettuata utilizzando protocolli di cifratura allo stato dell'arte, secondo le policy definite nei documenti accessori[8].

Nel caso di trattamento di dati genetici, deve essere garantita, oltre alle disposizioni previste dal GDPR, la normativa nazionale di attuazione. A tale scopo, il trattamento di dati genetici, anche a fini di ricerca, viene autorizzato solo su infrastrutture ed a personale esplicitamente qualificati. Le infrastrutture INFN a questo dedicate devono essere qualificate tramite certificazioni standard ISO.

[8] https://security.infn.it/computing-rules/policy-crittografia

9.7 Accesso urgente ed improrogabile ad informazioni di servizio

Qualora fosse necessario ed improrogabile accedere a dati o messaggi inerenti l'attività lavorativa in possesso esclusivo dell'utente, e solo in caso di prolungata irreperibilità o grave impedimento, il direttore di riferimento o un suo delegato può accedere ai dati e messaggi dell'utente per individuare ed estrarre le informazioni rilevanti per lo svolgimento dell'attività lavorativa.

Di questa attività verrà redatto un verbale e l'utente verrà informato se e appena possibile.

9.8 Scadenza del rapporto di lavoro o collaborazione

Alla cessazione del rapporto di lavoro o di collaborazione l'accesso alle risorse informatiche viene revocato. Entro tale termine l'utente ha il dovere di rendere disponibili i dati di collaborazione ai colleghi e di trasferire altrove i dati personali.

Su richiesta dell'utente il direttore di riferimento può autorizzare una estensione dell'accesso per un periodo massimo di due mesi al solo scopo di completare questi trasferimenti.

Entro il termine di 12 mesi dalla cessazione del rapporto di lavoro o collaborazione, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente.

In caso di grave indisponibilità o decesso dell'utente, il Direttore di riferimento, su richiesta, potrà rendere disponibile agli aventi diritto i dati con contenuti personali nelle ipotesi e secondo le modalità previste dalla normativa vigente.

10. Dispositivi mobili

L'uso di dispositivi mobili comporta specifici rischi legati alla loro portabilità e al loro utilizzo anche per uso privato.

L'INFN adotta le misure necessarie ad ottemperare agli obblighi del presente Disciplinare sui dispositivi mobili di proprietà dell'Ente (COPE). L'utente assegnatario del dispositivo COPE è ritenuto responsabile di eventuali danni cagionati per un uso negligente o nel caso abbia ridotto o eliminato le misure di sicurezza adottate dall'Ente.

Al fine di tutelare la privacy dei dipendenti, la sicurezza delle infrastrutture dell'Ente e dei dati trattati in relazione all'attività lavorativa, l'uso di dispositivi mobili personali (BYOD) per finalità connesse all'attività lavorativa è consentito esclusivamente previa accettazione e osservanza delle politiche specifiche in materia di gestione dei dispositivi, di sicurezza dei dati e delle reti, delle modalità accettabili di utilizzo, del backup e del ripristino dei dati[9].

11. 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, previa apposita informativa da rendere ai sensi del GDPR, adotta misure che consentono la verifica di comportamenti anomali o delle condotte non consentite dal presente Disciplinare, nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine, il team responsabile delle risorse informatiche o il NUCS possono eseguire elaborazioni sui dati registrati per rilevare anomalie nel traffico di rete o condotte non consentite.

Nel caso in cui si verifichino eventi dannosi o si rilevino comportamenti non consentiti, il team

[9] https://security.infn.it/computing-rules/dispositivi-mobili

responsabile delle risorse informatiche o il NUCS eseguono, previa informazione agli interessati e salvo i casi di necessità e urgenza, ulteriori accertamenti e adottano le misure necessarie ad interrompere le condotte dannose o non consentite.

Nei casi di reiterazione di comportamenti vietati o di particolare gravità, il team responsabile delle risorse informatiche adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al direttore di riferimento, che dispone gli ulteriori provvedimenti ai sensi del paragrafo "**Violazione delle norme**".

12. Violazione delle norme

Ogni condotta attuata in violazione del presente Disciplinare potrà determinare la sospensione dell'accesso alle risorse informatiche, 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 l'esercizio del diritto di rivalsa nei confronti del responsabile, nelle forme e limiti stabiliti dalla legge.

13. Disposizioni finali

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

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 elettronica o cartacea, idonee comunque a dimostrarne l'avvenuta consegna.

I documenti accessori citati nei paragrafi precedenti, oltre ad altri che si possano rendere necessari a seguito delle evoluzioni tecnologiche, costituiscono parte integrante del presente Disciplinare.

Tali documenti sono aggiornati dalla Commissione Calcolo e Reti di concerto con il Responsabile della Transizione Digitale e sono disponibili all'indirizzo: https://security.infn.it/computing-rules.

14. Clausola di revisione

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

Password policy all'INFN

CCR_SEC_01
Rev. 01 - 24/08/2025

Questo documento definisce le caratteristiche minime di sicurezza che devono essere rispettate nella creazione e gestione delle password degli utenti dei sistemi informatici dell'INFN, al fine di proteggere al meglio gli account e i dati degli utenti e le risorse informatiche INFN.

Ove possibile queste caratteristiche devono essere supportate dalle interfacce di selezione delle password per aiutare gli utenti al loro rispetto.

1. La password utilizzata sull'account INFN deve essere diversa dalle password utilizzate dall'utente per l'accesso ad altri servizi esterni all'INFN quali piattaforme social, caselle di posta personali, piattaforme commerciali, account presso altre Istituzioni, etc...

2. La password è una sequenza di caratteri che deve soddisfare i seguenti requisiti:
   i. lunghezza di almeno 10 caratteri;
   ii. presenza di almeno 3 classi di caratteri tra:
      - Lettere minuscole: abcdefghijklmnopqrstuvwxyz
      - Lettere maiuscole: ABCDEFGHIJKLMNOPQRSTUVWXYZ
      - Cifre numeriche: 0123456789
      - Simboli di punteggiatura: ,:;?!
      - Caratteri speciali: -_+*#@^=|\"£$%&/()§°çòàùéèì[]{}€<>
   iii. la password deve avere validità massima di 1 anno e minima di 1 giorno;
   iv. la password selezionata deve essere diversa dalle ultime 5 password utilizzate dall'utente;
   v. la password non deve essere banale (sequenze dello stesso carattere o di tasti adiacenti sulla tastiera), presente in dizionari, costituita da dati personali dell'account (combinazioni banali di nome/cognome);

3. La password non deve mai essere salvata in forma non criptata su supporti elettronici o cartacei.

4. Le credenziali di accesso ai sistemi INFN sono strettamente personali: la password non deve mai essere comunicata a nessuno.

Formazione sulla sicurezza informatica

CCR_SEC_02
Rev. 02 - 28/09/2025

Per ottenere un accesso alle risorse informatiche dell'INFN i richiedenti devono sostenere un corso di formazione sulla sicurezza informatica di livello adeguato alla criticità delle risorse ed al livello di privilegio richiesto.

I corsi di formazione possono essere effettuali in presenza o usufruiti online. In ogni caso deve essere previsto un test finale di superamento del corso.

Nel caso in cui l'accesso sia consentito a soggetti esterni all'INFN, la formazione in sicurezza informatica può essere certificata dall'Organizzazione di afferenza, nelle modalità specificate nel Disciplinare per l'utilizzo delle risorse informatiche dell'INFN.

Questo documento definisce i contenuti minimi che devono essere trattati nella formazione di sicurezza nei diversi casi.

Corso di formazione di sicurezza informatica di base

Tutti coloro che richiedono un accesso alle risorse informatiche dell'INFN devono seguire un corso di formazione di sicurezza di base.

L'INFN mette a disposizione dei propri utenti un corso di formazione di base fruibile online, dietro autenticazione INFN, al seguente link:

https://elearning.infn.it/course/view.php?id=105

Il corso tratta i seguenti argomenti:

1. Obblighi, norme d'uso ed informazioni generali
   problematica generale e aggiornamento sugli attuali obblighi di legge riguardanti gli utilizzatori di risorse informatiche dell'INFN
2. Protezione dei propri dispositivi informatici
   protezione dei propri dispositivi da accessi non autorizzati
3. E-mail e Web
   problematiche di sicurezza legate all'uso della posta elettronica e alla navigazione sul web, inclusi attacchi di social engineering (ad es.: phishing)
4. Password
   scelta, gestione e protezione delle proprie credenziali di accesso
5. Protezione dei file e dei dati

indicazioni per garantire la protezione dei propri dati depositati su device o su storage esterno

6. Copyright e file sharing
   sensibilizzazione sui concetti di copyright e proprietà intellettuale e sulle possibili conseguenze della loro violazione.
7. Stimolo delle sensibilità personali alle problematiche di sicurezza informatica
   Stimolo alla consapevolezza dell'importanza delle informazioni che vengono acquisite e trattate nel lavoro quotidiano

Il corso di formazione è oggetto di revisione ciclica in funzione della evoluzione delle tecnologie e delle problematiche connesse. In caso di revisione, sarà richiesto agli utenti di fruire obbligatoriamente del corso nella nuova versione.

Disposizioni per l'utilizzo di servizi esterni per ospitare o trattare dati e documenti dell'INFN

CCR_SEC_03
Rev. 01 - 24/08/2025

Questo documento indica i criteri in base ai quali gli utenti di risorse informatiche dell'INFN possono utilizzare per la loro attività servizi esterni, inclusi servizi cloud e piattaforme di Intelligenza Artificiale, in funzione della tipologia di dati trattati, per garantire la necessaria riservatezza anche ai fini del trattamento dei dati personali conforme alla disciplina del GDPR.

1. Indicazioni generali

Ove possibile, è sempre preferibile trattare dati utilizzando uno dei servizi interni dell'INFN quali: Alfresco (docs.infn.it), Pandora (pandora.infn.it), INFN GitLab (baltig.infn.it), INFN wiki (confluence.infn.it, wiki.infn.it), etc., o l'utilizzo di applicativi, anche sviluppati esternamente, ma installati su risorse INFN.

Nella scelta di affidarsi ad un servizio esterno è sempre a carico degli utenti considerare con la dovuta attenzione i seguenti aspetti:

- è indispensabile garantire l'accesso ai propri dati per tutto il tempo necessario, anche a lungo termine;
- è necessario valutare le condizioni contrattuali in relazione alla proprietà intellettuale ed ai relativi diritti nell'utilizzo dei dati e delle informazioni esposte;
- è necessario evitare un lock-in, e quindi pianificare una procedura per il recupero dei dati dalla piattaforma esterna in caso di dismissione del servizio

Qualsiasi servizio erogato da fornitore esterno ed utilizzato per attività gestionali o amministrative deve essere certificato dalla Agenzia per la Cybersicurezza Nazionale. Il catalogo dei servizi certificati è consultabile sul sito di ACN[1].

Prima di effettuare qualsiasi acquisto di servizi esterni è necessario consultare il Team responsabile delle risorse informatiche di riferimento, il rappresentante locale in Commissione Calcolo e Reti o l'Ufficio Transizione Digitale, per accertarsi della compatibilità del servizio proposto e verificare che l'esigenza non sia già fruibile attraverso soluzioni sviluppate internamente o su servizi esterni già acquistati centralmente dall'INFN.

2. Dati ordinari

[1] https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

Si intendono dati sostanzialmente pubblici, quali i dati di esperimento o collaborazione, che non abbiano particolari requisiti di riservatezza ed in cui il contenuto di dati personali ordinari sia trascurabile.

Fatto salvo quanto indicato nel paragrafo "**Indicazioni generali**", per questo tipo di dato non ci sono particolari prescrizioni. È utilizzabile qualsiasi risorsa esterna, di collaborazione o commerciale, anche ad uso gratuito.

Esempi:

- strumenti gestiti da organizzazioni con cui l'INFN ha accordi di collaborazione: CERN, EGI, ...
- strumenti e servizi cloud commerciali, anche quando utilizzati in forma gratuita, quali ad esempio i servizi offerti da Amazon, Google, Microsoft, DropBox, GitLab, etc.

È autorizzata l'elaborazione di documenti contenenti tale tipologia di dati con sistemi esterni di intelligenza artificiale, quali ad esempio OpenAI ChatGPT o Microsoft Copilot, anche in forma gratuita.

3. Dati scientifici riservati

Si intendono dati di tipo tecnico-scientifico che rivestono carattere di riservatezza. Esempi sono:

- dati di esperimento non ancora resi aperti, ad es. dati sotto embargo o con licenza chiusa
- draft di pubblicazioni scientifiche di particolare rilevanza
- progetti tecnologici in attesa di brevetto
- dati coperti da accordi di NDA
- codice sorgente, anche parziale, coperto da una qualsiasi forma di licenza di riutilizzo o comunque di proprietà dell'INFN

Questi dati possono essere trattati su servizi esterni, sia commerciali che non commerciali, per i quali esista un contratto di servizio o un accordo di collaborazione che garantisca il rispetto della riservatezza.

Attualmente i servizi esterni autorizzati sono:

- Piattaforma Office365 su tenant INFN (Microsoft SharePoint, Teams, OneDrive, etc.)
- In caso di dati di proprietà di una collaborazione scientifica, sono autorizzati eventuali sistemi di storage esterni autorizzati dalla collaborazione stessa;

È autorizzata l'elaborazione di documenti contenenti tale tipologia di dati con i seguenti sistemi di intelligenza artificiale:

- Microsoft Copilot in versione licenziata su tenant INFN

Non è consentita l'elaborazione su sistemi esterni di intelligenza artificiale diversi da quelli indicati, inclusa la versione Copilot su tenant INFN priva di licenza.

È responsabilità dell'utente adottare le misure necessarie a garantire la protezione dei dati adottando configurazioni di permessi o condivisione di link di accesso appropriati.

È necessario considerare le caratteristiche dei servizi utilizzati e mantenere il controllo dei dati in termini di protezione e disponibilità.
In caso di dati condivisi da uffici o collaborazioni è altamente sconsigliato l'utilizzo di aree private, anche in cloud (ad esempio OneDrive); si suggerisce piuttosto di usare aree condivise (ad esempio SharePoint) per evitare la perdita di dati al momento della chiusura di un account.

È altresì necessario che le aree in cloud esterne siano utilizzate solo per la fase di elaborazione di dati e documenti e non per l'eventuale conservazione a lungo termine, per la quale è disponibile il sistema documentale dell'ente, fornito di sistema di backup.

4. Dati personali e dati particolari non genetici

Si intendono i dati in cui sia rilevante la componente di dati personali ordinari, o che contengono dati personali particolari non genetici.

Esempi sono:

- documenti di commissioni di concorso
- documenti connessi a procedure di procurement
- documenti gestiti dalle Direzioni di AC
- documenti gestiti dai servizi del personale
- documenti gestiti dai servizi di prevenzione e protezione
- dati relativi ad accounting e monitoring sull'utilizzo dei sistemi informatici dell'INFN da parte degli utenti di tali sistemi
- dati trattati per garantire la sicurezza dei sistemi informatici dell'INFN, quali quelli relativi all'end point protection, alla threat analysis, etc.

La gestione di questi dati richiede il rispetto delle norme relative al GDPR, che possono essere garantite solo da servizi interni o da servizi esterni contrattualizzati e che siano certificati come idonei ad ospitare servizi cloud per la Pubblica Amministrazione o per i quali sia stata fatta una valutazione del rischio che verifichi 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 e i profili di responsabilità nel trattamento e definito la qualificazione dei rapporti in relazione alla disciplina del GDPR.

Per garantire il più elevato grado di sicurezza, questi dati devono essere conservati su sistemi interni all'Ente o tramite l'utilizzo di applicativi, anche sviluppati esternamente, ma installati su risorse INFN.

È consentito l'utilizzo di servizi esterni, comunque qualificati come sopra descritto, solo per motivi di necessità, quali l'esternalizzazione di un servizio (es: stipendiale, end point protection), o la condivisione in fase di elaborazione dei dati con strumenti o in ambiti non coperti dai sistemi interni.
È responsabilità dell'utente adottare le misure necessarie a garantire la protezione

dei dati adottando configurazioni di permessi o condivisione di link di accesso appropriati.

Si richiede comunque che i dati vengano rimossi dalla piattaforma esterna al termine della fase di elaborazione, e depositati per l'archiviazione a lungo termine su sistemi interni quali ad esempio Alfresco (https://docs.infn.it).

I servizi cloud esterni attualmente autorizzati sono:

- Zucchetti (limitatamente allo stipendiale)
- Piattaforma Office365 su tenant INFN (SharePoint, Teams, ...)
- Microsoft End Point Protection (solo su tenant INFN)

L'utilizzo di Microsoft OneDrive o altre aree personali per dati e documenti condivisi da uffici o collaborazioni è fortemente sconsigliato per gli stessi motivi indicati precedentemente.

È autorizzata l'elaborazione di documenti contenenti tale tipologia di dati con i seguenti sistemi di intelligenza artificiale:

- Microsoft Copilot in versione licenziata, su tenant INFN

Non è consentita l'elaborazione su sistemi esterni di intelligenza artificiale diversi da quelli indicati, inclusa la versione Copilot su tenant INFN priva di licenza.

5. Dati genetici

Nel caso di trattamento di dati genetici deve essere garantita, oltre alle disposizioni previste dal GDPR, la normativa nazionale di attuazione.

A tale scopo, il trattamento su servizi esterni di dati genetici, anche a fini di ricerca, può essere autorizzato solo su infrastrutture o servizi cloud **esplicitamente qualificati allo scopo**, tramite certificazioni o dichiarazioni di idoneità emesse dalle istituzioni nazionali preposte (ACN).

Non è consentito il trattamento di dati genetici su piattaforme esterne di intelligenza artificiale, anche se coperte da contratto INFN.

Dispositivi mobili

CCR_SEC_04
Rev. 01 24/08/2025

Questo documento stabilisce prescrizioni o linee guida per l'utilizzo di strumenti informatici di tipo mobile (smartphone, tablet, portatili) di proprietà personale o di terzi (BYOD) o forniti dall'INFN (COPE) per accedere a risorse informatiche dell'INFN.

L'obiettivo è di preservare la sicurezza informatica, la conformità al disciplinare e l'utilizzo responsabile delle risorse informatiche dell'INFN, garantendo al contempo la massima flessibilità per il lavoro delle persone.

1. Ambito

Il presente Disciplinare si applica a tutti coloro cui sia stato consentito l'accesso alle risorse informatiche dell'INFN e che accedono a tali risorse attraverso l'uso di dispositivi COPE o BYOD.

2. Disposizioni generali

È consentito l'utilizzo di dispositivi BYOD per svolgere attività lavorative, inclusi l'accesso alla posta elettronica, a documenti e servizi, alle reti wired e wireless delle strutture, nel rispetto delle linee guida sotto riportate.

I dispositivi COPE possono essere utilizzati per attività personali nei limiti descritti nel disciplinare di utilizzo delle risorse informatiche dell'INFN.

Nell'uso dei dispositivi COPE (sempre) e dei dispositivi BYOD quando connessi alle reti INFN (cablata, wireless o tramite VPN) è obbligatorio rispettare integralmente le prescrizioni riportate nel disciplinare di utilizzo delle risorse informatiche dell'INFN, in particolare in relazione al divieto di svolgere attività illegali o contrarie alle consuetudini d'uso delle reti e servizi acceduti o attività che possano nuocere alla reputazione dell'Ente.

Ove non esplicitamente indicato, le seguenti disposizioni vanno intese come obbligatorie per i dispositivi COPE, e come linee guida consigliate per i dispositivi BYOD.

3. **Protezione del dispositivo**

- non è consentito creare utenze oltre a quella personale sul dispositivo;
  nel caso di dispositivo BYOD è fortemente sconsigliata la creazione di altre utenze privilegiate;
- l'account non deve essere condiviso (obbligatorio anche per dispositivi BYOD).
- l'accesso al dispositivo deve essere protetto da password o da PIN adeguatamente complessi o da autenticazione biometrica (obbligatorio anche per dispositivi BYOD);
- l'accesso al dispositivo deve essere bloccato se lasciato incustodito, e deve essere configurata la modalità di blocco automatico per inattività (obbligatorio anche per dispositivi BYOD);
- il furto o la perdita del dispositivo COPE devono essere immediatamente segnalati al team responsabile delle risorse informatiche di riferimento;
  nel caso di dispositivi BYOD la segnalazione deve essere fatta solo se il dispositivo è stato registrato per la connessione diretta alle reti INFN

4. Sicurezza del sistema e del software

- Il sistema operativo e le app installate sul dispositivo devono essere sempre aggiornati all'ultima release disponibile;
- l'installazione delle app deve avvenire da repository certificati, come ad esempio, Apple Store, Windows Store e Google Play;
- il dispositivo COPE deve essere associato alla piattaforma di protezione Microsoft XDR dell'INFN secondo le istruzioni del team responsabile delle risorse informatiche di riferimento;
  sul dispositivo BYOD è fortemente consigliata l'installazione di uno strumento di protezione da virus/malware;
- non è consentito aggirare le configurazioni di sicurezza del dispositivo;

5. Sicurezza dei dati

- sul dispositivo ove possibile deve essere configurata la criptazione del disco e dei dati;
- l'accesso a dati e documenti INFN deve essere fatto esclusivamente utilizzando protocolli o app sicuri (obbligatorio anche per BYOD);
- non è consentito salvare documenti e dati INFN su cloud esterne non autorizzate (obbligatorio anche per BYOD);
- è consentito salvare copie di backup del dispositivo e di dati e configurazioni ivi contenuti solo in forma criptata end-to-end;
  se il backup del dispositivo include dati, documenti o credenziali INFN, la disposizione è obbligatoria anche per dispositivi BYOD;

6. Accesso alla rete

- È sconsigliato l'utilizzo di reti wireless non crittografate per accedere a risorse dell'INFN; in caso di necessità è consentito farne uso a patto di attivare una connessione VPN messa a disposizione dall'INFN o di utilizzare per l'accesso a risorse INFN esclusivamente protocoli criptati
- L'accesso a reti locali cablate è consentito solo previa identificazione del dispositivo (es: registrazione del MAC address) o dell'utente (es: 802.1X), secondo le procedure definite dal team responsabile delle risorse informatiche di riferimento (anche per device BYOD);

Policy per l'utilizzo e la gestione delle tecniche crittografiche

CCR_SEC_05
Rev. 02 26/10/2025

1. Scopo

La presente policy definisce i principi e le regole per l'uso della crittografia all'interno dell'organizzazione al fine di:

- Garantire la riservatezza, l'integrità e l'autenticità delle informazioni trattate;
- Proteggere informazioni e comunicazioni, con particolare riferimento ai dati considerati critici (da qui in poi: *dati riservati*) in relazione all'operatività dell'organizzazione (per esempio: dati personali particolari ai sensi del GDPR, generici dati sensibili in relazione all'eventuale classificazione in vigore);
- Assicurare la conformità alle vigenti normative e linee guida in materia.

2. Ambito di applicazione

La presente policy si applica a tutti i sistemi e servizi informatici dell'INFN che trattano *dati riservati* ai fini dell'operatività dell'organizzazione stessa; elenca e distingue obblighi, prescrizioni e buone pratiche per:

- Amministratori di Sistema e utenti privilegiati
- Utenti ordinari - dipendenti, associati, ospiti e visitatori

3. Principi generali

L'utilizzo della crittografia deve conformarsi in ogni caso ai seguenti principi di base:

- **Necessità e proporzionalità** – La crittografia deve essere applicata in funzione del livello di rischio e della eventuale classificazione delle informazioni;
- **Utilizzo di algoritmi riconosciuti** – Devono essere utilizzati solo algoritmi e protocolli crittografici riconosciuti da standard internazionali e da questi classificati come sicuri;
- **Sicurezza delle chiavi** – la chiavi crittografiche (certificati X.509 personali e per server/servizi; chiavi SSH; chiavi per la crittografia di dati e documenti) sono da considerarsi elementi critici per la sicurezza dell'organizzazione e vanno generate,

gestite e protette adeguatamente seguendo, se necessario, le prescrizioni elencate nel seguito.

4. Disposizioni generali

Protezione dei dati a riposo

- è raccomandata la cifratura dei dischi di server e workstation ospitanti *dati riservati*; è obbligatoria la cifratura dei dischi di dispositivi mobili contenenti *dati riservati*;
- è obbligatoria la cifratura di *dati riservati* che risiedano su cloud esterne non autorizzate; le chiavi di cifratura non devono risiedere sugli stessi dispositivi che contengono i dati a cui sono riferite;
- le chiavi crittografiche devono, ove richiesto, essere protette da passphrase non banali e vanno conservate su dispositivi sicuri e non in aree condivise via rete a meno che ciò non sia indispensabile per l'operatività dei servizi.

Protezione dei dati in transito

- è obbligatorio utilizzare esclusivamente protocolli (TLS) o applicativi (ssh, VPN) sicuri per servizi che espongono *dati riservati* (anche tramite API) o richiedono accesso autenticato (portali web, spedizione e lettura posta elettronica, accesso interattivo);
- le chiavi crittografiche non devono essere trasmesse su canali in chiaro;
- eventuali servizi legacy di accesso in chiaro a dispositivi e apparecchiature che per motivi tecnici non supportino protocolli sicuri devono obbligatoriamente essere esposti solo su rete privata e protetti adeguatamente con firewall perimetrali o locali; è vietato esporre su rete geografica servizi che utilizzano protocolli di accesso con autenticazione in chiaro (telnet, ftp, http autenticato);
- è obbligatorio utilizzare la crittografia end-to-end per la trasmissione di *dati riservati* mediante posta elettronica;
- per l'accesso da reti pubbliche non sicure a risorse e servizi dell'INFN è obbligatorio utilizzare i servizi VPN messi a disposizione dai team responsabili delle risorse informatiche delle strutture o utilizzare esclusivamente protocolli di rete criptati.

Protezione dei backup:

- è raccomandato cifrare i supporti di backup/archiviazione o utilizzare applicazioni di backup che permettano la cifratura dei dati;
- è obbligatorio cifrare i backup prima di trasferirli via rete, o utilizzare protocolli di trasmissione cifrati;
- è obbligatorio cifrare i backup se ospitati su servizi cloud esterni.

5. Disposizioni per Amministratori di Sistema e Utenti privilegiati

5.1. Implementazione di SSL/TLS

Gestione di certificati e chiavi private

- Le chiavi vanno generate su un sistema affidabile e possibilmente isolato e dotato di sufficiente entropia;
- le chiavi RSA devono avere dimensione non inferiore a 2048 bit; per applicazioni particolarmente critiche è opportuno considerare l'utilizzo di chiavi RSA da 3072 bit o, ove le prestazioni siano importanti, chiavi ECDSA da 256 bit o più;
- l'algoritmo di hashing della firma deve essere almeno SHA256;
- per servizi esposti all'utenza è obbligatorio utilizzare solo certificati emessi da CA pubbliche, ed è obbligatorio provvedere al rinnovo tempestivo dei certificati in scadenza;
  per tali servizi non è consentito l'utilizzo di certificati *self-signed*.

Protocolli ammessi e configurazioni consigliate

- L'utilizzo di **SSL v2** e **SSL v3** (entrambi insicuri e obsoleti) è **esplicitamente proibito;**
- **TLS v1.0** e **TLS v1.1** sono da considerarsi protocolli legacy, sono stati ufficialmente deprecati nel gennaio del 2020 e **non dovrebbero essere usati;**
- **TLS v1.2** e **TLS v1.3** non presentano problemi di sicurezza noti e **dovrebbero essere i principali o, ancora meglio, gli unici protocolli supportati.**
- Utilizzare solo suite di cifratura sicure (meglio se con selezione da parte del server), Perfect Forward Secrecy (PFS) e protocolli di scambio chiavi forti (Strong Key Exchange): per i dettagli fare riferimento ai documenti della serie "Linee Guida Funzioni Crittografiche" pubblicati da ACN[1];
- verificare periodicamente le configurazioni dei servizi esposti utilizzando scanner TLS (testssl.sh, SSL Server Test by Qualys)

5.2. Configurazione dei server ssh

SSH, la cui versione minima **deve** essere la 2.0, supporta diversi 1) algoritmi di scambio di chiavi, 2) algoritmi di cifratura e 3) codici di autenticazione dei messaggi per garantire autenticità, confidenzialità e integrità delle comunicazioni tra server e client: gli algoritmi obsoleti, poco sicuri o sospettati di compromissione vanno disabilitati anche correndo il rischio di risultare incompatibili con clienti obsoleti. Per valutare la sicurezza della configurazione dei server SSH esposti si raccomanda di utilizzare il tool di audit 'ssh-audit' (https://github.com/jtesta/ssh-audit, https://www.sshaudit.com/) e di applicare le relative *hardening guide*.

5.3. Configurazione dei server di posta elettronica

Per i mail server autenticati e i server per l'accesso alle caselle di posta fare riferimento a quanto già prescritto per la configurazione di SSL/TLS, avendo cura di proibire l'accesso ai

[1] https://www.acn.gov.it/portale/crittografia

servizi in chiaro; è consigliabile implementare il *TLS opportunistico* anche sugli MTA in modo da garantire – ove possibile - la massima sicurezza delle comunicazioni mantenendo la interoperabilità con gli MTA che non supportano la crittografia.

6. Disposizioni per gli utenti

Gestione di certificati e chiavi private

Le chiavi dei certificati RSA devono avere dimensione non inferiore a 2048 bit ma è consigliabile richiedere già oggi l'emissione di certificati RSA con chiavi di dimensione maggiore (3072 o 4096 bit) o, se supportati dai sistemi nei quali verranno impiegati, di certificati con chiavi ECDSA da 128 o 256 bit.

Gestione delle chiavi private SSH

Le chiavi attualmente utilizzate per l'autenticazione su SSH che offrono il miglior compromesso in termini di sicurezza e prestazioni sono le classiche chiavi RSA e le più recenti chiavi EdDSA basate su curve ellittiche; le prime devono avere dimensione non inferiore a 2048 bit, equivalenti a una sicurezza pari a 112 bit (ma il default sui sistemi Redhat-like di versione uguale o superiore a 9 è 3072 bit, equivalenti a 128 bit), mentre le chiavi basate su curve ellittiche hanno lunghezza fissa.

Crittografia end-to-end

È obbligatorio utilizzare la crittografia end-to-end per la trasmissione di *dati sensibili*; questa prescrizione è particolarmente stringente nel caso della posta elettronica, poiché è in grado di garantire la confidenzialità sul lungo periodo anche delle caselle di posta.

Utilizzo di reti wireless pubbliche; VPN

È sconsigliato l'utilizzo di reti wireless pubbliche in chiaro (cioè non crittografate) per accedere a risorse dell'organizzazione; in caso di necessità è consentito farne uso a patto di utilizzare esclusivamente protocolli criptati per l'accesso a dati e servizi INFN o di attivare la connessione VPN messa a disposizione dalla struttura di riferimento.

Norme d'uso
per sistemi operativi Linux

V 2.0 – 15/10/2025

Contents

1. Introduzione

Questa guida riporta procedure, azioni e configurazioni volte all'attuazione di quanto richiesto dalla Circolare AgID (Agenzia per l'Italia Digitale) 18/04/2017, n. 2/2017 "**Misure minime di sicurezza ICT per le pubbliche amministrazioni** (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)", GU Serie Generale n.103 del 05-05-2017), dal **Regolamento Generale sulla Protezione dei Dati (GDPR)**, recepito in Italia con il D.lgs. 101/2018, dalla recente **Direttiva NIS2**, recepita in Italia con il D.lgs. 138/2024 ed, infine, dal **Disciplinare per l'uso delle risorse informatiche dell'INFN**.

2. Le raccomandazioni per l'utilizzo dei device personali

I possessori di un account amministrativo di uno o piu device personali, possono limitarsi a seguire le raccomandazioni incluse in questo capitolo. Coloro che siano stati nominati "amministratori di sistema" dovranno implementare tutte le misure incluse nel documento.
Con il termine "device personali" si intendono i desktop/laptop assegnati agli utenti nell'ambito della loro attività lavorativa e sui quali non sono presenti account di altri utenti e non sono presenti in maniera continuativa dati riservati. Per questi dispositivi non è necessaria la nomina di amministratore di sistema da parte del Direttore di riferimento.

1. Utilizzare sistemi operativi per i quali attualmente è garantito il supporto e autorizzati dal Team responsabile delle risorse informatiche di riferimento. (vedi capitolo 4)

2. Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo (vedi capitolo 6.a)

3. Assicurarsi che i software di protezione del sistema operativo (firewall, antimalware, ecc) siano abilitati e costantemente aggiornati (vedi capitolo 5, 9 e 14)

4. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alla password policy adottate dall'INFN

5. Non installare software proveniente da fonti/repository non ufficiali, per i quali non si è provvisti di adeguata licenza o espressamente vietati dal Team responsabile delle risorse informatiche di riferimento.

6. Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro

7. Non cliccare su link o allegati contenuti in email sospette, applicare adeguate misure sulla difesa dai malware (vedi capitolo 9)

8. Collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dal team responsabile delle risorse informatiche di riferimento)

9. Configurare la criptazione dei disco sui portatili; configurare la criptazione del disco sui desktop che ospitino dati riservati o personali (vedi capitolo 11)

3. Responsabilità dell'amministratore di sistema

Le procedure, azioni e configurazioni volte all'attuazione di quanto richiesto limitatamente al solo livello minimo di sicurezza, saranno indicate con le seguenti parole chiave e incluse in un rettangolo (nel caso di misure richieste solamente per sistemi multiutente il fondo sarà grigio):

È OBBLIGATORIO,
DEVE / DEVONO,
SI DEVE / SI DEVONO.

Sarà compito e responsabilità dell'amministratore del sistema attuare quanto indicato.

Tutte le indicazioni non individuate dalle parole chiave di sopra sono suggerimenti non previsti esplicitamente nel livello minimo di sicurezza della Circolare, ma comunque consigliati per migliorare la sicurezza del sistema.

4. Installazione e configurazione del sistema operativo

Al fine di utilizzare configurazioni sicure standard per la protezione dei sistemi operativi si consiglia di coordinare con il Team responsabile delle risorse di calcolo di riferimento la fase di installazione e configurazione di sistemi operativi GNU/Linux, secondo le modalità stabilite dal Team stesso.

Si consiglia di non collegare alla rete sistemi preinstallati o dei quali non si conosce in dettaglio la configurazione.

Se l'accesso fisico alla macchina non è controllato, si consiglia di

- impostare una password per accedere al BIOS,
- disabilitare nel *BIOS* il boot da dispositivi esterni,
- impostare una password nel *boot loader* (per es. **grub**).

a. Installazione

Se non si utilizza un sistema di installazione semiautomatica predisposto dal Team responsabile delle risorse di calcolo di riferimento, **SI DEVONO** utilizzare per l'installazione solamente immagini prelevate dai *repository* ufficiali o fornite dal Team, verificandone il *check-sum* con quello riportato nel *repository*.

Se si impiegano immagini virtuali, *container* o *docker* preconfezionati le credenziali di amministrazione **DEVONO** essere modificate prima del collegamento alla rete.[1]

Se l'immagine di installazione non è stata fornita dal Team responsabile delle risorse di calcolo di riferimento, **DEVE** essere salvata su supporti conservati *offline*.

Installare solo versioni supportate e stabili evitando di usare versioni obsolete o di test. Nel caso si renda necessario mantenere in produzione sistemi non aggiornabili, **DEVONO** essere applicate misure di mitigazione del rischio come, ad esempio, isolare il dispositivo dal resto della rete.

Si consiglia di verificare periodicamente la data di EOL del sistema operativo attraverso fonti autorevoli quali, ad esempio, il sito del produttore o aggregatori on line (es.: https://endoflife.date/)

Nel caso di server, eseguire un'installazione minimale del sistema operativo, non installando software non strettamente necessario al funzionamento dei servizi offerti.

Nel caso di server con servizi centralizzati **È OBBLIGATORIO** compilare e mantenere aggiornato l'elenco dei software utilizzati e le loro versioni.

In accordo con quanto indicato nel *Disciplinare per l'uso delle risorse informati- che*, gli indirizzi IP utilizzati **DEVONO** essere assegnati dal Team responsabile delle risorse di calcolo di rifermento (direttamente o tramite server DHCP).

b. Configurazione e primo avvio

Le password di tutte le utenze amministrative:

- **DEVONO** rispettare la password policy adottata dall'INFN

1 Ad esempio disabilitando l'interfaccia di rete e collegandosi come amministratore alla console virtuale.

Ogni forma di login come root al di fuori delle *virtual console* (tty*), incluso l'accesso via **ssh**, **DEVE** essere disabilitata.

Si consiglia di eseguire le seguenti operazioni al primo avvio:

- assicurarsi che il sistema di gestione dei pacchetti verifichi le *signature* dei pacchetti tramite **gpg**, in modo da ridurre la possibilità di installare pacchetti sospetti;
- chiudere tutti i servizi non strettamente necessari ed evitarne l'avvio in fase di boot; in particolare per i portatili disattivare il *bluetooth service,* attivandolo solo in caso di necessità;
- se non necessari rimuovere i seguenti utenti: adm, ftp, games, gopher, halt, lp, mail, news, operator, shutdown, userdel, uucp;
- se non necessari rimuovere i seguenti gruppi: adm, dip, games, groupdel, lp, mail, news, uucp;
- disabilitare gli account speciali (per es. nobody, sync) necessari per il funzionamento del sistema modificandone la *shell* in /etc/passwd in /bin/false;
- verificare che venga richiesta la password di root quando si avvia il sistema in modalità single-user; in caso diverso, provvedere a forzare la richiesta di autenticazione anche in in modalità single-user, soprattutto se alla macchina possono aver accesso fisico non controllato persone diverse;
- controllare l'accesso a servizi e risorse da parte di indirizzi specifici tramite regole nftables, firewalld;
- controllare l'accesso a servizi e risorse da parte di utenti specifici tramite le librerie PAM (ad esempio pam_access tramite il file /etc/security/access.conf) o sistemi di autorizzazione centralizzata via SSSD.

c. Condivisione di filesystem

- Nel caso sia necessario condividere un filesystem (via CIFS, NFS, ecc..) seguire le seguenti indicazioni
- impedire l'accesso a **root** (se possibile)[2];

2 La richiesta è molto forte e praticamente inapplicabile nella maggior parte dei casi. Valutarne comunque la fattibilità per migliorare la protezione contro ransomware (Reveton,

CryptoLocker, WannaCry, ...).

- montare il flesystem in read-only (se possibile);
- limitare sempre l'esposizione del filesystem ai soli host necessari;
- controllare la situazione degli accessi periodicamente (ad esempio, per NFS, con il comando showmount);
- nel caso in cui il filesystem sia inserito in **/etc/fstab** usare l'opzione nosuid;
- se possibile filtrare le porte di accesso permettendo l'accesso ai soli dispositivi previsti,tramite un firewall (ad es. Nftables o Firewalld);

5. Accesso remoto al sistema

Per accedere da remoto al sistema **SI DEVE** impiegare solo software che utilizza protocolli sicuri (per es. **ssh**, **scp**, **rdp**, **vnc over tls**).

Per semplifcare i processi di autenticazione e autorizzazione, alcuni servizi e applicazioni permettono di configurare macchine remote come macchine "fidate", dalle quali è possibile accedere direttamente al servizio o applicazione anche in modo non interattivo. La configurazione di queste relazioni di fiducia è in generale sconsigliata.

L'accesso remoto automatico a scopo di configurazione o altre operazioni va garantito attraverso meccanismi di chiave asimmetrica, limitandolo solo agli ip previsti.

.

6. Manutenzione

a. Aggiornamento del sistema

Il sistema **DEVE** essere mantenuto costantemente aggiornato. In particolare, **SI DEVONO** applicare tutte le patch di sicurezza appena disponibili. Per far questo possono essere impostati aggiornamenti automatici (p.e. tramite cron) sia per i pacchetti presenti nella distribuzione sia per il software esterno.

Se non si ritiene opportuno l'uso degli aggiornamenti automatici, deve comunque essere previsto un sistema di allarme che verifichi la disponibilità di aggiornamenti. In questo caso **È OBBLIGATORIO** attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare, le patch **DEVONO** essere applicate a partire da quelle più critiche.

A seguito di modifiche significative del sistema (p.e. aggiunta di nuovi servizi), **È OBBLIGATORIO** concordare con il Team responsabile delle risorse di calcolo di riferimento l'esecuzione di una scansione di sicurezza per individuare eventuali ulteriori vulnerabilità. A scansione avvenuta, **DEVONO** essere intraprese tutte le azioni necessarie per risolvere le vulnerabilità accertate o, qualora non sia possibile, documentare il rischio accettato, dandone anche comunicazione al Servizio Calcolo.

b. Verifica degli account e delle credenziali

Si consiglia di eseguire periodicamente controlli con programmi specifici sugli account utente. John the Ripper rimane uno strumento utile per il controllo della robustezza delle password in ambienti Linux e Unix. Dal 2025, la sua versione Jumbo supporta hash moderni e GPU acceleration. Tuttavia, strumenti come Hashcat, Hydra e Patator offrono funzionalità avanzate per il controllo distribuito, online e su protocolli specifici.

7. Gestione degli utenti

I privilegi di amministrazione **DEVONO** essere limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

È OBBLIGATORIO mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

Le utenze amministrative **DEVONO** essere utilizzate solamente per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. A tal fine **È OBBLIGATORIO** utilizzare sempre *sudo* per eseguire comandi di amministrazione.

È OBBLIGATORIO assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali **DEVONO** corrispondere credenziali diverse. In altre parole, se un utente di un sistema ha an- che il ruolo di amministratore di tale sistema, avrà due account differenti di cui solo uno facente parte del gruppo *sudoers* da usare per eseguire comandi di am- ministrazione.

È OBBLIGATORIO che tutte le utenze, in particolare quelle amministrative, debbano essere nominative e riconducibili ad una sola persona.

È OBBLIGATORIO che tutte le utenze create siano autorizzate secondo il Disciplinare per l'uso delle risorse informatiche dell'INFN.

8. Gestione di file con dati critici o “rilevanti” per l'ente

File che contengono dati con particolari requisiti di riservatezza (dati rilevanti per l'ente) o informazioni critiche come certifcati personali, certifcati server, chiavi private **ssh**, chiavi **gpg**, ecc... **DEVONO** essere archiviati con permessi 600 (rw- --- ---) o 400 (r-- --- ---).

Si consiglia di cifrare le chiavi private con password (ad esempio via openssl), mantenerla su filesystem cifrato (LUKS, ext4 fscrypt) e possibilmente utilizzare chiavi differenti per utenze di servizio differenti.

9. Difese contro i malware

È OBBLIGATORIO installare e configurare opportunamente sistemi anti-malware integrati (ad es. Microsoft EDR/XDR, Wazuh XDR, ecc..)

È OBBLIGATORIO l'uso di un *firewall* (ad esempio Nftables o Firewalld) .

È OBBLIGATORIO limitare l'uso di dispositivi esterni riducendone il loro utilizzo esclusivamente alle situazioni strettamente necessarie allo svolgimento della pro- pria attività lavorativa

Si consiglia di disattivare l'apertura automatica dei messaggi di posta elettronica e l'anteprima automatica dei contenuti dei file.

10. Copie di sicurezza

È OBBLIGATORIO effettuare almeno settimanalmente una copia di sicurezza delle "informazioni strettamente necessarie per il completo ripristino del sistema".

Nel caso di backup su Cloud o nel caso in cui non sia possibile assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione, assicurandosi che il sito di backup non sia accessibile in modo permanente via rete, onde evitare che attacchi al sistema possano coinvolgere anche tutte le sue copie di sicurezza.

11. Protezione dei dati tramite crittografia

Per i portatili si consiglia l'uso di un filesystem cifrato, consigliabile anche per le postazioni fisse su cui siano presenti dati che richiedono particolari requisiti di riservatezza. Si raccomanda di abilitare la cifratura al momento dell'installazione di sistema operativo.

Rispettare le indicazioni dell'Ente sulle tipologie di file che **DEVONO** essere protetti tramite cifratura, avendo l'accortezza di proteggere adeguatamente le chiavi private .

12. Compromissione del sistema

In caso di compromissione del sistema il Team responsabile delle risorse di calcolo di riferimento **DEVE** essere immediatamente informato. Il ripristino del sistema **DEVE** essere eseguito tramite le immagini salvate a con- clusione della fase di installazione e confgurazione o come una nuova installazio- ne.

13. File di log

L'analisi periodica dei file di log è una pratica che aiuta a risolvere problemi di sicurezza, oltre che di errata configurazione del sistema.

Si raccomanda quindi di adeguare il livello di logging di ogni macchina e la durata della conservazione dei log in base alla criticità del sistema nei limiti definiti dal disciplinare.

Dove possibile, si raccomanda di mantenere una copia dei messaggi su di un'altra macchina (logging remoto).

14. Altre raccomandazioni

Non utilizzare script setuid, ma usare sempre sudo.
Installare software per il controllo dell'integrità dei file di sistema come, ad esempio, *ossec* o *AIDE*.

Si raccomanda di filtrare tutti i servizi di sistma tranne quelli necessari.

E' **PROIBITO** attivare sistemi di posta elettronica. L'amministratore di sistema **DEVE** concordare l'attivazione di servizi web con il team responsabile delle risorse informatiche di riferimento

Controlli periodici a titolo di esempio:

- Verificare che le interfacce di rete (sia ethernet che wireless) non siano in modo promiscuo.
- Verificare che i device /dev/mem e /dev/kmem non siano leggibili a tutti gli utenti.
- Verificare che tutti i devices siano dell'utente root ad eccezione dei terminali.
- Verificare che non siano presenti file "normali" (*regular file*) nella directory /dev.
- Installare software per il controllo dell'integrità dei file di sistema (File Integrity Monitoring) come, ad esempio, *ossec*.
- Verificare la presenza di file con il bit SUIG/SGID abilitato:

  `find / -type f \( -perm -04000 –o –perm -02000 \) –exec ls –l {} \;`
- Verificare la presenza di file con il nome insolito, come ad esempio "..." (tre punti) o ".. " (punto punto spazio) o "..^G" (punto punto control-G):

  `find / -name ".. " –print –xdev`

  `find / -name ".*" –print –xdev | cat -v`
- Verificare la presenza di file e directory scrivibili al mondo:

  `find / -type f \( -perm -2 –o –perm -20 \) –exec ls –lg {} \; find / -type d \( -perm -2 –o –perm -20 \) –exec ls –ldg {} \;`
- Verificare la presenza di file che non appartengono a nessuno (tralasciando ciò che viene riportato eventualmente dalla directory /dev):

```
find / -nouser –o -nogroup
```

- Verifiicare la presenza di fle .rhosts; se è necessario che esistano, verificare perlomeno che non contengano wildcard o righe di commento.
- Verificare gli *umask* degli utenti (quello di root sia almeno 0x22).

Norme d'uso
per sistemi operativi Windows

v 2.0 – 01/10/2025

Sommario

Introduzione

Questa guida riporta procedure, azioni e configurazioni volte all'attuazione di quanto richiesto nella Circolare AgID (Agenzia per l'Italia Digitale) 18/04/2017, n. 2/2017 “Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)”, GU Serie Generale n.103 del 05-05-2017), dal Regolamento Generale sulla Protezione dei Dati (GDPR), recepito in Italia con il D.lgs. 101/2018, dalla recente Direttiva NIS2, recepita in Italia con il D.lgs. 138/2024 ed, infine, dal Disciplinare per l'uso delle risorse informatiche dell'INFN..

Responsabilità dell'amministratore di sistema

Le procedure, azioni e configurazioni volte all'attuazione di quanto richiesto nella Circolare AgID limitatamente al solo livello minimo di sicurezza, saranno indicate con le seguenti parole chiave e incluse in un rettangolo (nel caso di misure richieste solamente per sistemi multiutente il fondo sarà grigio):

È OBBLIGATORIO, DEVE / DEVONO, [NON] SI DEVE / [NON] SI DEVONO.

Sarà compito e responsabilità dell'amministratore del sistema attuare quanto indicato. Gli obblighi indicati nel paragrafo **Gestione degli utenti** si applicano solo ai sistemi multiutente.

Tutte le indicazioni non individuate dalle parole chiave di sopra sono suggerimenti non previsti esplicitamente nel livello minimo di sicurezza della Circolare, ma comunque consigliati per migliorare la sicurezza del sistema.

Installazione e configurazione del sistema operativo

Al fine di utilizzare configurazioni sicure standard per la protezione dei sistemi operativi [ABSC ID 3.1.1, 3.2.1] la fase di installazione e configurazione di sistemi operativi Windows deve essere coordinata con i Servizi di Calcolo presenti nell'Unità Operativa, secondo le modalità stabilite dai Servizi stessi, oltre a quelle riportate in questa guida.

Evitare di collegare alla rete sistemi preinstallati o dei quali non si conosce in dettaglio la configurazione.

Nel caso si utilizzino immagini virtuali o preconfigurazioni, le credenziali di amministrazione DEVONO essere modificate prima di collegare il sistema alla rete.

Se la macchina opererà in un ambiente dove hanno libero accesso fisico studenti o altre persone non soggette alla politica di sicurezza informatica dell'INFN, si consiglia di

- impostare una password per accedere al *BIOS*,
- disabilitare nel *BIOS* il boot da *floppy*, da *CD* o da *USB.*
- Abilitare Secure Boot.

Installazione

Se non è possibile utilizzare un sistema di installazione semiautomatica predisposto dal Team responsabile delle risorse informatiche di riferimento, **SI DEVONO** utilizzare per l'installazione solamente immagini prelevate dai *repository* ufficiali o fornite dal Team, verificandone il *checksum* con quello riportato nel *repository*.

Se l'immagine di installazione non è stata fornita dal Team, **DEVE** essere salvata su supporti conservati *offline*.

Installare solo versioni supportate e stabili evitando di usare versioni obsolete, non più mantenute o versioni di test.

Nel caso di server con servizi centralizzati **È OBBLIGATORIO** compilare e mantenere aggiornato l'elenco dei software utilizzati e le loro versioni.

In accordo con il "Disciplinare per l'uso delle risorse informatiche", per quanto riguarda la configurazione di rete, nel caso di reti in cui sia presente un DHCP server, configurare i sistemi per ottenere la configurazione di rete tramite tale servizio; nel caso di IP statici, utilizzare solo gli indirizzi IP a loro assegnati dal Team responsabile de.lle risorse informatiche di riferimento

In ogni caso **NON SI DEVONO** utilizzare indirizzi IP arbitrari non assegnati dai Team(sia assegnati all'utente che tramite DHCP).

Configurazione e primo avvio

Al fine di aumentare la sicurezza del sistema operativo si consiglia di eseguire le seguenti operazioni al primo avvio, possibilmente scollegati dalla rete.

Versione del sistema operativo

Nel caso di utilizzo di un portatile o desktop è proibito l'utilizzo delle versioni Home di Windows, in quanto non supportate dalla piattaforma di endpoint protection di Microsoft

Nome del computer

Il nome del computer (hostname, computer name,…) deve essere concordato con il Team responsabile delle risorse informatiche di riferimento al fine di agevolarne l'identificazione.

Nome utente

Nel corso della prima configurazione viene richiesto un account Microsoft si consiglia invece di impostare un account locale selezionando "Opzioni di accesso" ("Sign-in options") e quindi "Aggiungi a un dominio" ("Domain join instead").

Impostare la verifica delle *signature* dei pacchetti

Assicurarsi che il sistema di gestione dei pacchetti verifichi le *signature* dei pacchetti in modo da ridurre la possibilità di installare pacchetti sospetti.

Rimozione dei pacchetti non necessari

Al fine di ridurre il numero di software potenzialmente vulnerabile si consiglia di eliminare tutti i pacchetti che non siano strettamente necessari al sistema operativo, ai servizi e agli strumenti utilizzati.

Creare vincoli sulle password

SI DEVONO impostare Group Policy in modo da richiedere che le credenziali delle utenze amministrative siano aderenti alla password policy definita dall'Ente.

Blocco di account speciali

Laddove possibile **SI DEVE** lasciare l'account **Administrator** disabilitato e creare un altro account con i privilegi amministrativi, da usare solo in casi eccezionali, con una username non significativa (p. es, non nominarlo: **root**, **amministratore, superuser**)

Accesso a servizi da parte di utenti specifici

È possibile controllare (impedire, limitare e monitorare) l'accesso a servizi e risorse da parte di utenti specifici tramite Group Policy

Accesso a porte o servizi specifici tramite rete

È possibile controllare (impedire, limitare e monitorare) l'accesso a specifiche porte e servizi configurando opportunamente il firewall.

È proibito attivare servizi di posta elettronica o messaggistica eventuali altri servizi come ad esempio un web server DEVONO essere concordati con il Team responsabile delle risorse informatiche.

Condivisione di file

Se è necessario condividere file o cartelle del proprio PC si raccomanda di configurare correttamente lo *sharing* impostando almeno le seguenti restrizioni:

- Impedire lo sharing verso **everyone;**
- permettere lo *sharing* solo al ristretto gruppo di persone che ne dovranno fare uso impostando gli opportuni permessi (read/write, read…)

Accesso remoto al sistema

L'accesso da remoto al sistema **DEVE** avvenire solo tramite RDP (Remote Desktop Connection) con la funzione Network Level Authentication abilitata, specificando opportunamente gli account che potranno eseguirlo.

Manutenzione

Aggiornamento del sistema

Il sistema operativo **DEVE** esser mantenuto costantemente aggiornato. In particolare, si **DEVONO** applicare tutte le *patch* di sicurezza appena si rendono disponibili. Si suggerisce di abilitare gli aggiornamenti automatici sia per il sistema operativo sia per il software installato.

Qualora sul sistema siano presenti servizi critici che potrebbero interrompersi in seguito ad aggiornamenti automatici **DEVE** comunque esser previsto un sistema di allarmistica che verifichi la disponibilità di aggiornamenti da essere eseguiti con procedure interattive quanto prima. In tal caso **SI DEVE** attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare, SI DEVONO applicare le patch per le vulnerabilità a partire da quelle più critiche.

Qualora non sia possibile risolvere le vulnerabilità accertate **SI DEVE** documentare il rischio accettato , dandone anche comunicazione al Team responsabile delle risorse informatiche di riferimento.

A seguito di modifiche significative del sistema (p.e. aggiunta di nuovi servizi), **È OBBLIGATORIO** concordare con il Team l'esecuzione di una scansione di sicurezza per individuare eventuali ulteriori vulnerabilità. A scansione avvenuta, **DEVONO** essere intraprese tutte le azioni necessarie per risolvere le vulnerabilità accertate o, qualora non sia possibile, documentare il rischio accettato, dandone anche comunicazione al Team.

Verifica degli account e delle credenziali

Al fine di verificare la robustezza delle credenziali amministrative si consiglia d'impostare le opportune *group policy* (lunghezza minima, complessità) ed eseguire periodicamente controlli con programmi specifici sui file di password degli account utente.

Gestione degli utenti

Tutte le utenze create su un dispositivo DEVONO essere autorizzate secondo il Disciplinare per l'uso delle risorse informatiche dell'INFN.

Si **DEVONO** Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

DEVE essere mantenuto l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

Le utenze amministrative **DEVONO** essere utilizzate solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.

DEVE essere assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. In altre parole, se un utente di un sistema ha anche il ruolo di amministratore di tale sistema, avrà due account differenti di cui solo uno facente parte del gruppo **Administrators** da usare per eseguire comandi di amministrazione.
Tutte le utenze, in particolare quelle amministrative, DEVONO essere nominative e riconducibili ad una sola persona.

Gestione di file con dati critici o “rilevanti” per l'ente

L'accesso a file che contengono dati con particolari requisiti di riservatezza (dati rilevanti per l'ente) o informazioni critiche come certificati personali, certificati server, chiavi private **ssh**, chiavi **gpg**, ecc... **DEVE** essere limitato al solo proprietario.

Difese contro i malware

DEVE essere installato l'agente di endpoint protection messo a disposizione dall'ente impostando l'aggiornamento automatico e l'esecuzione automatica delle scansioni anti-malware dei supporti rimovibili al momento della loro connessione.

È OBBLIGATORIO l'uso di un firewall personale e le funzionalità IPS dell'agente **DEVONO** essere attivate

È OBBLIGATORIO limitare l'uso di dispositivi esterni riducendone il loro utilizzo esclusivamente alle situazioni strettamente necessarie allo svolgimento della propria attività lavorativa.

È OBBLIGATORIO disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili (Autoplay).

È OBBLIGATORIO disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.

È OBBLIGATORIO disattivare l'apertura automatica dei messaggi di posta elettronica.

È OBBLIGATORIO disattivare l'anteprima automatica dei contenuti dei file.

Copie di sicurezza

È OBBLIGATORIO effettuare almeno settimanalmente una copia di sicurezza delle "informazioni strettamente necessarie per il completo ripristino del sistema". In particolare su sistemi che contengono i dati degli utenti (home directory, dati amministrativi,…).

Nel caso di backup su Cloud, o nel caso in cui non sia possibile assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti, **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione, assicurandosi che non siano accessibile in modo permanente via rete, onde evitare che attacchi al sistema possano coinvolgere anche tutte le sue copie di sicurezza[1].

Protezione dei dati tramite crittografia

Per i portatili si consiglia l'uso di un *filesystem* criptato (BitLocker) in modo che, in caso di smarrimento, i dati in esso contenuto non siano accessibili a nessuno.

L'uso del *filesystem* criptato è consigliabile anche per le postazioni fisse su cui siano presenti dati che richiedono particolari requisiti di riservatezza.

Rispettare le indicazioni dell'Ente sulle tipologie di file che **DEVONO** essere protetti tramite cifratura, avendo l'accortezza di proteggere adeguatamente le chiavi private.

Compromissione del sistema

In caso di compromissione del sistema informare immediatamente il Team responsabile delle risorse informatiche di riferimento e concordare con esso la procedura di ripristino.

Il ripristino del sistema **DEVE** essere eseguito tramite le immagini salvate a conclusione della fase di installazione e configurazione del sistema o come una nuova installazione[2].

1. La richiesta è volta a migliorare la protezione contro ransomware (Reveton, CryptoLocker, WannaCry, …).
2. Vedi "Installazione".

File di log

Il mantenimento e l'analisi periodica dei file di log rappresentano pratiche che possono aiutare a risolvere problemi di sicurezza oltre che di mal configurazione dei sistemi.

Si raccomanda di mantenere una copia dei messaggi di logging, dove possibile, su di un'altra macchina.

Esempio di file di log da copiare su un'altra macchina:

- **%SystemRoot%\System32\Winevt\Logs\Application.evtx**
- **%SystemRoot%\System32\Winevt\Logs\Security.evtx**
- **%SystemRoot%\System32\Winevt\Logs\Setup.evtx**
- **%SystemRoot%\System32\Winevt\Logs\System.evtx**

Norme d'uso
per sistemi operativi Apple macOS

V 2.1 – 27/10/2025

Sommario

Introduzione

Questa guida riporta procedure, azioni e configurazioni volte all'attuazione di quanto richiesto dalla Circolare AgID (Agenzia per l'Italia Digitale) 18/04/2017, n. 2/2017 "**Misure minime di sicurezza ICT per le pubbliche amministrazioni** (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)", GU Serie Generale n.103 del 05-05-2017), dal **Regolamento Generale sulla Protezione dei Dati (GDPR)**, recepito in Italia con il D.lgs. 101/2018, dalla recente **Direttiva NIS2**, recepita in Italia con il D.lgs. 138/2024 ed, infine, dal **Disciplinare per l'uso delle risorse informatiche dell'INFN**.

2. Le raccomandazioni per l'utilizzo dei dispositivi personali

I possessori di un account amministrativo di uno o più dispositivi personali, possono limitarsi a seguire le raccomandazioni incluse in questo capitolo. Coloro che siano stati nominati "amministratori di sistema" dovranno implementare tutte le misure incluse nel documento.

Con il termine "dispositivi personali" si intendono i desktop/laptop assegnati agli utenti nell'ambito della loro attività lavorativa e sui quali non sono presenti account di altri utenti e non sono presenti in maniera continuativa dati riservati.

Per questi dispositivi non è necessaria la nomina di amministratore di sistema da parte del direttore della struttura, ma comunque l'assegnatario dovrà:

1. utilizzare sistemi operativi per i quali attualmente è garantito il supporto e autorizzati dal Team responsabile delle risorse informatiche di riferimento (vedi capitolo **Error! Reference source not found.**);

2. effettuare costantemente gli aggiornamenti del sistema operativo (vedi paragrafo 6a) ed applicare senza alcun indugio tutti gli aggiornamenti di sicurezza;

3. assicurarsi che i software di protezione del sistema operativo (Firewall, Antimalware, ecc.) siano abilitati e costantemente aggiornati (vedi capitolo 9);

4. assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy adottate dall'INFN;

5. non installare software proveniente da fonti/repository non ufficiali, per i quali non si è provvisti di adeguata licenza o espressamente vietati dal Team responsabile delle risorse informatiche di riferimento;

6. bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;

7. non cliccare su link o allegati contenuti in e-mail sospette, applicare adeguate misure sulla difesa dai malware (vedi capitolo 9);

8. collegare al dispositivo soltanto dispositivi mobili (pen-drive, hdd-esterno, ecc.) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dal Team responsabile delle risorse informatiche di riferimento);

9. assicurarsi che i laptop e desktop abbiano il disco criptato (vedi capitolo 11).

3. Responsabilità dell'amministratore di sistema

Le procedure, azioni e configurazioni volte all'attuazione di quanto richiesto limitatamente al solo livello minimo di sicurezza, saranno indicate con le seguenti parole chiave e incluse in un rettangolo (nel caso di misure richieste solamente per sistemi multiutente il fondo sarà grigio):

È OBBLIGATORIO,
DEVE / DEVONO,
SI DEVE / SI DEVONO.

Sarà compito e responsabilità dell'amministratore del sistema attuare quanto indicato.

Tutte le indicazioni non individuate dalle parole chiave di sopra sono suggerimenti non previsti esplicitamente nel livello minimo di sicurezza della Circolare, ma comunque consigliati per migliorare la sicurezza del sistema.

4. Installazione e configurazione del sistema operativo

Al fine di utilizzare configurazioni sicure standard per la protezione dei sistemi operativi si consiglia di coordinare con il Team responsabile delle risorse informatiche di riferimento la fase di installazione e configurazione di sistemi operativi macOS, secondo le modalità stabilite dal Team stesso.

Si consiglia di non collegare alla rete sistemi preinstallati o dei quali non si conosca in dettaglio la configurazione.

Se la macchina è accessibile ad altre persone oltre l'amministratore, si consiglia di impostare una password[1] per accedere al *Firmware* così da impedire l'avvio da dispositivi esterni e l'accesso alla Recovery Console.

[1] L'eventuale smarrimento della stessa richiede l'intervento di un centro assistenza Apple (https://support.apple.com/it-it/HT204455)

a. Installazione

Se non è possibile utilizzare un sistema di installazione semiautomatica predisposto dal Team responsabile delle risorse informatiche di riferimento, **SI DEVONO** utilizzare per l'installazione solamente immagini prelevate dai *repository* ufficiali Apple attraverso le procedure standard di Recovery o direttamente fornite dal Team responsabile delle risorse informatiche di riferimento.

Nel caso si utilizzino immagini virtuali, *container* o *docker* preconfezionati, le credenziali di amministrazione **DEVONO** essere modificate prima del collegamento alla rete

.

Installare solo versioni supportate e stabili, evitando di usare versioni obsolete e non più supportate da Apple.

Nel caso si renda necessario mantenere in produzione sistemi non aggiornabili, **DEVONO** essere applicate misure di mitigazione del rischio come, ad esempio,

Si consiglia di verificare periodicamente la data di EOL del sistema operativo attraverso fonti autorevoli quali, ad esempio, il sito del produttore o aggregatori on line (es.: https://endoflife.date/)

Nel caso di server, eseguire un'istallazione minimale del sistema operativo, non installando software che non sia strettamente necessario al funzionamento dei servizi offerti.

Nel caso di server con servizi centralizzati **È OBBLIGATORIO** compilare e mantenere aggiornato l'elenco dei software necessari e le loro versioni.

In accordo con quanto indicato nel *Disciplinare per l'uso delle risorse informatiche*, gli indirizzi IP utilizzati **DEVONO** essere assegnati dal Team responsabile delle risorse informatiche di riferimento (direttamente o tramite server DHCP).

b. Configurazione e primo avvio

Le password di tutte le utenze amministrative:

- **DEVONO** rispettare la password policy adottata dall'INFN.

Ogni forma di login come **root**, incluso l'accesso via **ssh**, **DEVE** essere disabilitata

Per accedere da remoto al sistema **SI DEVE** impiegare solo software che utilizzi protocolli sicuri (per es. *ssh*, *scp*, screen sharing solo con cifratura abilitata, ...)

Non utilizzare password “banali” o con parole presenti nei dizionari di qualsiasi lingua.

Per aumentare la sicurezza del sistema operativo si consiglia di eseguire le seguenti operazioni al primo avvio:

- disattivare il *bluetooth,* attivandolo solo in caso di necessità
- controllare (impedire, limitare e monitorare) l'accesso a servizi e risorse tramite le regole di Firewall

a. Condivisione di filesystem

Nel caso sia necessario condividere un filesystem, seguire le seguenti indicazioni

- impedire l’accesso a **root** (se possibile)[2]
- montare il flesystem in read-only (se possibile);
- limitare sempre l'esposizione del filesystem ai soli client necessari;
- controllare la situazione degli accessi periodicamente;
- se possibile filtrare le porte di accesso permettendo l’accesso ai soli dispositivi previsti, tramite un firewall.

5. Accesso remoto al sistema

Per accedere da remoto al sistema **SI DEVE** impiegare solo software che utilizza protocolli sicuri (per es. **ssh**, **scp**, **rdp**, **vnc over tls**).

Il sistema operativo macOS permette l’abilitazione della gestione remota. Se necessaria, questa dovrà essere adeguatamente configurata per impedire accessi non autorizzati.

[2] La richiesta è molto forte e praticamente inapplicabile nella maggior parte dei casi. Valutarne comunque la fattibilità per migliorare la protezione contro ransomware (Reveton, CryptoLocker, WannaCry, ...).

6. Manutenzione

a. Aggiornamento del sistema

Il sistema **DEVE** essere mantenuto costantemente aggiornato. In particolare, **SI DEVONO** applicare tutte le patch di sicurezza appena disponibili. Per far questo possono essere impostati aggiornamenti automatici tramite il servizio “aggiornamenti automatici” di Apple per i pacchetti presenti nella distribuzione ufficiale, mentre per il SW aggiuntivo esterno all’App Store occorre utilizzare meccanismi manuali o basati su sistemi MDM centralizzati.

Se non si ritiene opportuno l'uso degli aggiornamenti automatici, deve comunque essere previsto un sistema di allarme che verifichi la disponibilità di aggiornamenti. In questo caso **È OBBLIGATORIO** attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare, le patch **DEVONO** essere applicate a partire da quelle più critiche.

A seguito di modifiche significative del sistema (p.e. aggiunta di nuovi servizi), **È OBBLIGATORIO** concordare con il Team responsabile delle risorse informatiche di riferimento l'esecuzione di una scansione di sicurezza per individuare eventuali ulteriori vulnerabilità. A scansione avvenuta, **DEVONO** essere intraprese tutte le azioni necessarie per risolvere le vulnerabilità accertate o, qualora non sia possibile, documentare il rischio accettato, dandone anche comunicazione al Team responsabile delle risorse informatiche di riferimento.

7. Gestione degli utenti

I privilegi di amministrazione **DEVONO** essere limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

È OBBLIGATORIO mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

Le utenze amministrative **DEVONO** essere utilizzate solamente per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. A tal fine **È OBBLIGATORIO** utilizzare sempre *sudo* per eseguire comandi di amministrazione.

È OBBLIGATORIO assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali **DEVONO** corrispondere credenziali diverse. In altre parole, se un utente di un sistema ha anche il ruolo di amministratore di tale sistema, avrà due account differenti di cui solo uno con privilegi amministrativi da usare per eseguire comandi di amministrazione.

È OBBLIGATORIO che tutte le utenze, in particolare quelle amministrative, debbano essere nominative e riconducibili ad una sola persona.

È OBBLIGATORIO che tutte le utenze create siano autorizzate secondo il Disciplinare per l'uso delle risorse informatiche dell'INFN.

Dalla versione macOS El Capitan in poi ogni utente con diritti **Admin** è nel gruppo dei sudoers e l'utente root è disabilitato. È inoltre attivo un meccanismo che impedisce anche agli utenti con privilegi di root di effettuare modifiche considerate pericolose (System Integrity Protection).

È comunque consigliabile, quando possibile, distinguere l'utenza amministrativa da quella di uso comune, ricorrendo all'uso del comando **sudo** per ridurre il rischio di eseguire operazioni dannose per il sistema.

8. Gestione di file con dati critici o rilevanti per l'ente

File che contengono dati con particolari requisiti di riservatezza (dati rilevanti per l'ente) o informazioni critiche come certificati personali, certificati server, chiavi private **ssh**, chiavi **gpg**, ecc... **DEVONO** essere archiviati con permessi 600 (rw- --- ---) o 400 (r-- --- ---).

9. Difese contro i malware

È OBBLIGATORIO installare e configurare opportunamente sistemi anti-malware integrati (ad es. Microsoft EDR/XDR, Wazuh XDR, ecc..)

È OBBLIGATORIO abilitare e configurare il *firewall integrato o sistema equivalente*

È OBBLIGATORIO limitare l'uso di dispositivi esterni riducendone il loro utilizzo esclusivamente alle situazioni strettamente necessarie allo svolgimento della propria attività lavorativa

Si consiglia di disattivare l'apertura automatica dei messaggi di posta elettronica e l'anteprima automatica dei contenuti dei file.

10. Copie di sicurezza

È OBBLIGATORIO effettuare almeno settimanalmente una copia di sicurezza delle "informazioni strettamente necessarie per il completo ripristino del sistema" per esempio utilizzando la time machine su disco esterno o network filesystem avendo cura di abilitare la cifratura.

Nel caso di backup su Cloud o nel caso in cui non sia possibile assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione, assicurandosi che il sito di backup non sia accessibile in modo permanente via rete, onde evitare che attacchi al sistema possano coinvolgere anche tutte le sue copie di sicurezza.

11. Protezione dei dati tramite crittografia

Per i portatili si consiglia l'uso di un filesystem cifrato abilitando il *FileVault*, consigliabile anche per le postazioni fisse su cui siano presenti dati che richiedono particolari requisiti di riservatezza.

Rispettare le indicazioni dell'Ente sulle tipologie di file che **DEVONO** essere protetti tramite cifratura, avendo l'accortezza di proteggere adeguatamente le chiavi private .

12. Compromissione del sistema

In caso di compromissione del sistema il Team responsabile delle risorse di calcolo di riferimento **DEVE** essere immediatamente informato. Il ripristino del sistema **DEVE** essere eseguito tramite le immagini salvate a conclusione della fase di installazione e configurazione o come una nuova installazione.

13. File di log

L'analisi periodica dei file di log è una pratica che può aiutare a risolvere problemi di sicurezza, oltre che di mal configurazione del sistema.

Si raccomanda quindi di adeguare il livello di logging di ogni macchina e la durata della conservazione dei log in base alla criticità del sistema nei limiti definiti dal disciplinare.

Dove possibile, si raccomanda di mantenere una copia dei messaggi su di un'altra macchina (logging remoto).

14. Difese Altre raccomandazioni

- Si consiglia di installare software per il controllo dell'integrità dei file di sistema in aggiunta al controllo previsto dal sistema operativo.

- Si consiglia di analizzare sistematicamente la compliance alle policy di security proposte dagli organismi di certificazione (CIS,NIST,SANS,etc)

E' **PROIBITO** attivare sistemi di posta elettronica.

L'amministratore di sistema **DEVE** concordare l'attivazione di servizi web con il team responsabile delle risorse informatiche di riferimento

Norme per il trattamento di dati personali nell'INFN

4 Dicembre 2018

PREMESSA

Questo documento contiene le istruzioni per il trattamento dei dati personali nell'Istituto Nazionale di Fisica Nucleare (di seguito anche INFN) in conformità a quanto disposto:

- dal Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (di seguito anche Regolamento);
- dal Codice in materia di trattamento dei dati personali di cui al D.Lgs. n. 196/2003 e ss.mm.ii. recante disposizioni per l'adeguamento nazionale al Regolamento UE n. 2016/679 (di seguito anche Codice).

Il personale dipendente ed associato, nonché tutti coloro che collaborano a qualunque titolo nelle attività dell'INFN che comportino il trattamento di dati personali, sono tenuti ad osservarle, conformando la propria condotta a criteri di diligenza e correttezza, al fine di assicurare la massima tutela ai dati trattati.

DEFINIZIONI

Si intende per

- **Dato Personale:** qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamen-

te, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

- **Categorie particolari di dati personali:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati relativi a condanne penali e reati:** dati relativi a vicende riguardanti persone fisiche disciplinate dalla legislazione penale, nonché la comminatoria di misure di sicurezza.
- **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

PRINCIPI GENERALI

Il trattamento di dati personali deve essere effettuato nel rispetto dei principi di:

- liceità, correttezza e trasparenza;
- limitazione della finalità del trattamento, assicurando che eventuali trattamenti successivi non siano incompatibili con le finalità per le quali i dati sono stati raccolti;
- minimizzazione dei dati, prestando cura che i dati siano adeguati, pertinenti e limitati a quanto necessario per raggiungere le finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione di quelli che risultino inesatti rispetto alle finalità del trattamento;

- limitazione della conservazione, limitando la conservazione dei dati a un periodo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza, garantendo un'adeguata sicurezza dei dati personali oggetto del trattamento.

I SOGGETTI

I soggetti rilevanti nella disciplina in materia di trattamento dei dati personali sono:

- il Titolare,
- il Responsabile per la protezione dei dati personali,
- i Responsabili del trattamento (eventuali),
- gli Autorizzati al trattamento,
- gli Interessati al trattamento.

Titolare del trattamento dei dati personali: è l'Istituto Nazionale di Fisica Nucleare, cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali. Con deliberazione n. 14844 del 27 luglio 2018 il Consiglio Direttivo dell'INFN ha attribuito:

- al Direttore Generale funzioni di coordinamento per l'attuazione della disciplina in materia di trattamento dei dati personali, assegnandogli, in particolare, il compito di fornire indicazioni di carattere generale, emanare direttive, definire modelli standard delle informative, degli atti di designazione e delle istruzioni, nonché dei contratti di designazione dei Responsabili esterni al trattamento, coordinare la definizione delle misure tecniche ed organizzative volte ad assicurare all'interno dell'INFN il corretto adempimento del Regolamento e la concreta applicazione delle indicazioni provenienti dall'Autorità di controllo;
- ai Direttori delle Strutture dell'INFN, in considerazione dell'attuale organizzazione dei sistemi informativi, il compito di attuare le misure tecniche di sicurezza contenute nell'allegato alla medesima deliberazione, integrandole, se del caso, per assicurare un più efficace livello di sicurezza dei dati personali all'interno della Struttura che dirigono; di assicurare, su base permanente, la riservatezza, la disponibilità e la resilienza dei sistemi esistenti nella Struttura, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la predisposizione e l'esecuzione con rego-

larità di procedure per verificare e valutare l'efficacia delle misure adottate;

- al Direttore Generale, ai Direttori delle Strutture, ai Direttori delle Aree, Direzioni, Divisioni e Servizi Professionali dell'Amministrazione Centrale, di cui all'art. 2 del Disciplinare Organizzativo dell'Amministrazione Centrale, nonché ai Responsabili del Servizio di Presidenza e dell'Ufficio Comunicazione, negli ambiti di rispettiva competenza definiti dagli atti interni dell'Istituto, il compito di assicurare il rispetto di tutti gli obblighi previsti dal Regolamento e dalla normativa nazionale in capo al Titolare del trattamento ed in particolare di provvedere alla effettiva e concreta attuazione delle misure tecniche ed organizzative volte a garantire e dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento presso ciascuna Struttura, articolazione o ufficio che dirigono o di cui hanno la responsabilità, quali:

  a) designare le persone autorizzate al trattamento dei dati personali nell'ambito della articolazione che dirigono; garantire che le stesse siano state preliminarmente istruite per il trattamento e si siano impegnate alla riservatezza; verificare l'osservanza delle istruzioni che sono state impartite per il trattamento, e, ove ne sussistano le condizioni, l'osservanza di obblighi legali di riservatezza;

  b) assicurare che l'informativa sul trattamento dei dati sia fornita all'interessato e, nei casi previsti, acquisirne il consenso;

  c) dar seguito alle eventuali richieste degli interessati per l'esercizio dei diritti loro garantiti dal Capo IV del Regolamento;

  d) implementare il Registro del trattamento dei dati personali, comunicando al DPO i nuovi trattamenti in uso presso la Struttura o l'articolazione che dirigono o di cui hanno la responsabilità;

  e) notificare al Garante della protezione dei dati personali le violazioni dei dati personali (data breach); provvedere alla comunicazione della violazione agli interessati, ai sensi degli articoli 33 e 34 del Regolamento, e darne informativa al Direttore Generale e al DPO;

  f) effettuare, quando sia necessaria e sentito il DPO, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali;

  g) mettere a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi richiesti dal Regolamento; consentire e contribuire alle attività di revisione e di ispezione;

  h) informare immediatamente il Direttore Generale e il DPO in ogni circostanza in cui ritengono che un'istruzione relativa al trattamento dei dati violi il Regolamento o altre disposizioni relative alla protezione dei dati;

i) designare quali Responsabili esterni al trattamento i soggetti che trattano dati personali per conto dell'INFN nell'ambito di convenzioni o contratti che hanno potere a sottoscrivere, nell'ambito delle competenze per valore e materia previste dagli atti interni dell'INFN;

j) individuare un referente locale quale punto di contatto con il DPO e supporto alle attività di gestione degli adempimenti connessi alla protezione dei dati.

Responsabile per la protezione dei dati personali o Data Protection Officier (DPO): è il soggetto designato con deliberazione n. 14734 del 27 aprile 2018 del Consiglio Direttivo dell'INFN, cui è attribuito il compito di:

a) informare e fornire consulenza al Titolare, ai Responsabili del trattamento nonché ai soggetti autorizzati al trattamento circa gli obblighi derivanti dal Regolamento e dalle norme nazionali ed europee relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento e delle altre norme relative alla protezione dei dati, ferme restando le responsabilità del Titolare e del Responsabile del trattamento.

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, pareri in merito alla valutazione di impatto sulla protezione dei dati (*Data Protection Impact Assesment,* DPIA) e sorvegliarne lo svolgimento: a tal proposito il Responsabile per la protezione dei dati indica la necessità di condurre la DPIA sulle singole categorie di trattamento, la metodologia da adottare, le salvaguardie da applicare, comprese le misure tecniche e organizzative per attenuare i rischi delle persone interessate, verificando inoltre se la DPIA sia stata condotta correttamente e se le conclusioni raggiunte siano conformi al Regolamento;

e) cooperare con il Garante per la protezione dei dati personali.

Il Responsabile per la protezione dei dati personali costituisce punto di contatto per gli interessati per tutte le questioni relative al trattamento dei dati personali nell'INFN ed all'esercizio dei diritti garantiti dal Regolamento.

Responsabile del trattamento: è ogni soggetto esterno all'INFN (persone fisiche, giuridiche, altre amministrazioni o autorità pubbliche o altri organismi) che tratta dati per conto dell'INFN.

L'Istituto Nazionale di Fisica Nucleare disciplina i rapporti con il Responsabile del trattamento mediante contratti o altri atti giuridici predisposti secondo i modelli individuati dal Direttore Generale, che vincolano il Responsabile del trattamento al Titolare e individuano l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del Titolare e del Responsabile del trattamento.

Autorizzati al trattamento: sono tutti coloro che agiscono sotto l'autorità del Titolare e che hanno accesso ai dati personali; i soggetti autorizzati al trattamento sono istruiti dal Titolare circa le modalità con le quali deve essere effettuato il trattamento.

Interessati al trattamento: sono coloro cui si riferiscono i dati personali trattati.

L'INFORMATIVA

Per adempiere agli obblighi di informazione sul trattamento di cui all'art. 13 del Regolamento, devono essere utilizzati gli schemi di informative disponibili al sito web del DPO dell'INFN.

Nello stesso sito è disponibile anche uno schema di informativa per il trattamento di dati ottenuti da soggetti diversi dai singoli interessati.

È necessario pertanto aver cura che all'avvio di ogni procedimento amministrativo o di qualunque altra attività che coinvolga il trattamento di dati personali sia fornita agli interessati, per iscritto e preferibilmente in formato elettronico, l'informazione preventiva circa:

- il Titolare del trattamento ed i relativi dati di contatto,
- i dati di contatto del Responsabile della Protezione dei dati,
- le finalità e modalità del trattamento,
- i legittimi interessi perseguiti dal Titolare,
- gli eventuali destinatari dei dati,
- l'eventuale trasferimento dei dati in un paese terzo o un'organizzazione internazionale,
- la natura obbligatoria o facoltativa del conferimento dei dati, con indicazione delle conseguenze di un eventuale rifiuto del conferimento stesso,
- il periodo di conservazione dei dati,
- il diritto di chiedere al Titolare l'accesso, la rettifica, o la cancellazione dei dati o la limitazione del trattamento, oltre il diritto di opporsi al loro trattamento,
- l'esistenza eventuale di processi decisionali automatizzati o di profilazione,
- il diritto di presentare un reclamo al Garante per la tutela dei dati personali.

COMUNICAZIONE E DIFFUSIONE DEI DATI

La comunicazione dei dati personali ad un altro soggetto pubblico può essere effettuata quando è prevista da una norma di legge o di regolamento o, in mancanza, se necessaria per lo svolgimento di compiti di interesse pubblico o di funzioni istituzionali, decorsi quarantacinque giorni dalla relativa comunicazione al Garante senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

La diffusione di dati personali trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri a soggetti che intendono trattarli per altre finalità è ammesso solo se previsto da norme di legge o di regolamento

L'art. 100 del Codice consente alle università e gli enti di ricerca, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, di adottare autonome determinazioni con le quali disporre la comunicazione o diffusione, anche a privati e per via telematica, di dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici, tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli di cui agli articoli 9 e 10 del Regolamento.

ISTRUZIONI PER IL TRATTAMENTO DI DATI PERSONALI

Regole generali

I soggetti autorizzati al trattamento devono:

- predisporre la modulistica per la raccolta dei dati personali avendo cura di chiedere agli interessati soltanto i dati necessari e pertinenti alla finalità per le quali sono raccolti;
- accertarsi che la raccolta dei dati personali sia giustificata da una effettiva base giuridica o comunque sia necessaria per eseguire compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è titolare l'INFN;
- nel caso in cui il dato che si intende raccogliere non sia giustificato da una effettiva base giuridica o non sia strettamente necessario per il raggiungimento di compiti di interesse pubblico, far sottoscrivere all'interessato una dichiarazione di consenso al trattamento;

- fornire agli interessati l'informativa sul trattamento in tutte le circostanze in cui procedono alla raccolta di dati personali;
- verificare l'esattezza della scritturazione o digitazione dei dati nelle operazioni di registrazione dei dati personali raccolti;
- utilizzare i dati personali in base al principio del *"need to know"* ed evitare di condividerli o comunicarli a persone che non ne hanno bisogno per lo svolgimento delle proprie mansioni lavorative;
- non trasmettere all'esterno o a soggetti terzi informazioni circa i dati personali conosciuti in ragione della propria attività, salvo che si tratti di comunicazione funzionale allo svolgimento dei propri compiti;
- conservare la riservatezza dei dati personali conosciuti nello svolgimento dell'attività lavorativa anche successivamente al trasferimento ad altra attività o nel periodo successivo alla cessazione del rapporto di lavoro;
- accertarsi dell'identità dell'interessato al momento della raccolta dei dati o prima di fornire informazioni circa i dati personali di altri interessati, anche ove la richiesta sia presentata nell'esercizio del diritto di accesso;
- nei casi in cui è ammessa la consultazione di dati personali e in particolare nei procedimenti di accesso a dati personali, verificare che i documenti oggetto di accesso non riportino dati particolari o dati relativi a condanne penali: in tal caso procedere all'oscuramento di tali informazioni (p. es. mediante *omissis*), salvo che non vi sia una base giuridica che autorizzi la conoscibilità anche di tale tipologia di dati;
- aver cura di non rendere conoscibili, neppure accidentalmente, a soggetti non autorizzati i dati personali contenuti in atti o documenti: a tal fine non lasciare in evidenza documenti quando si ricevono soggetti non autorizzati a conoscere tali dati o non lasciare aperto ed incustodito l'ufficio.

Trattamento con strumenti elettronici

Una buona attenzione alle regole elementari di sicurezza fisica è la base su cui poggiano tutte le altre regole. Per tale motivo è necessario osservare il Disciplinare per l'uso delle risorse informatiche dell'INFN ed in particolare aver cura di:

- accedere ai sistemi di gestione documentale informatizzata e alle banche dati contenenti dati personali soltanto attraverso le credenziali di accesso concesse dall'INFN e nei limiti delle abilitazioni operative consentite dall'Istituto;

- non utilizzare servizi cloud per il trattamento dei dati personali se non espressamente autorizzati dall'INFN;
- se si ha il sospetto che si sia verificato un accesso non autorizzato ai dati personali, segnalare immediatamente l'incidente al Direttore di Struttura o, per l'Amministrazione Centrale, al Direttore di Direzione, Divisione o Servizio di appartenenza;
- fare attenzione, nel caso in cui si utilizzino fotocopiatrici, stampanti o fax condivisi a non lasciare incustodito l'apparecchio con il quale vengono stampati, duplicati o ricevuti documenti contenenti dati personali e rimuovere immediatamente i documenti prodotti; nel caso in cui la stampante o la fotocopiatrice diano segnali di malfunzionamento provvedere a cancellare i lavori in coda, evitando che, a seguito di interventi di manutenzione, il macchinario proceda incustodito alla stampa di documenti contenenti dati personali;
- chiudere le applicazioni che si stavano usando, o attivare il salvaschermo protetto da password, quando si lascia la postazione di lavoro;
- se si trasferiscono dati personali su dispositivi rimovibili (p.e. chiavetta usb), avere cura di cancellarli al termine delle attività di trattamento.

Configurazione del sistema

Tutte le postazioni ed i dispositivi utilizzati per il trattamento di dati personali di cui è Titolare l'INFN devono essere dotati di un antivirus mantenuto costantemente aggiornato. Questo, però, non sempre garantisce una protezione completa (ad esempio per virus molto recenti); è essenziale quindi prestare molta attenzione ad ogni file che si intende aprire o link che si vuole seguire, **specialmente se ricevuti via posta elettronica**.

Le impostazioni del sistema fatte dal Servizio Calcolo non devono essere modificate senza un'autorizzazione preventiva. In particolare è necessario aver cura di:

- non permettere l'esecuzione automatica dei contenuti al momento dell'inserimento di un dispositivo rimovibile;
- attivare l'esecuzione delle macro eventualmente presenti nei file Office solo caso per caso, dopo aver verificato la loro indispensabilità;
- non attivare l'apertura automatica dei link esterni e degli allegati nei messaggi di posta elettronica;
- non attivare l'anteprima automatica dei contenuti dei file;
- non disattivare la scansione automatica anti-malware dei sispositivi rimovibili alla connessione.

Copie di salvataggio

Seguire le indicazioni del Servizio Calcolo in modo che i propri dati vengano salvati con regolarità.

Le password

La corretta individuazione, custodia e gestione delle password consente all'utente di tutelarsi rispetto ad eventuali attività non corrette o addirittura illecite effettuate da altri soggetti tramite il computer a lui assegnato.

La password è personale e l'utente è responsabile della corretta conservazione e gestione della stessa. Non deve essere comunicata ad altri né scritta su supporti facilmente accessibili a terzi. Nella sua scelta devono essere evitati riferimenti personali (nome e/o cognome proprio o di familiari, indirizzo ecc…), e preferite sequenze miste di caratteri e numeri.

I soggetti autorizzati al trattamento dei dati personali devono aver cura, inoltre, di non impiegare la stessa password per i diversi sistemi utilizzati e di non rendere note quelle non più in uso, perché potrebbero permettere l'individuazione delle regole adottate per la loro generazione.

Posta elettronica

I soggetti autorizzati al trattamento dei dati personali non devono mai fornire dati riservati via e-mail (ad es. password). I messaggi in cui vengono richieste informazioni di questo tipo, ad es. tramite un link ad una pagina, anche apparentemente legittima, sono sicuramente dei tentativi di phishing e vanno immediatamente segnalati al Servizio Calcolo.

Prima di aprire un link presente in un messaggio di posta elettronica, verificare con attenzione la sua legittimità, controllando ad esempio l'indirizzo visibile con quello che appare, di solito nella parte inferiore della finestra, quando vi si posiziona sopra il cursore.

Dismissione o reimpiego di apparecchiature elettroniche

I soggetti autorizzati al trattamento dei dati personali devono aver cura, nella dismissione o reimpiego di apparecchiature elettroniche che contengono dati personali, di attuare o far attuare tutte le misure tecniche volte a prevenire accessi non consentiti ai dati personali in esse contenuti mediante un'effettiva cancellazione che garantisca la loro non intelligibilità, secondo quanto disposto dal Garante per la tutela dei dati personali con Provvedimento del 13 ottobre 2008 ed annessi allegati.

Trattamento senza strumenti elettronici

Nel trattamento di dati personali effettuato senza strumenti elettronici (in modo analogico) i soggetti autorizzati al trattamento dei dati personali devono:

- conservare gli atti e i documenti contenenti dati personali soltanto per il tempo necessario alle attività da svolgere e riporli successivamente in archivi ad accesso controllato;
- non lasciare in evidenza sulla scrivania i documenti cartacei quando si ricevono soggetti non autorizzati a conoscere tali dati;
- chiudere a chiave l'ufficio quando ci si assenta;
- non lasciare gli atti e i documenti contenenti dati personali incustoditi su scrivanie o tavoli di lavoro e riporli nei relativi archivi ad accesso controllato a fine giornata;
- se si utilizza carta riciclata, verificare che i fogli non contengano sul retro dati personali;
- ove si renda necessario distruggere documenti contenenti dati personali, utilizzare gli apparecchi distruggi documenti o strapparli in porzioni tali da non essere ricomponibili.

RESPONSABILITÀ E SANZIONI

È riconosciuto il diritto al risarcimento a chiunque subisca un danno materiale o immateriale causato dalla violazione delle norme del Regolamento. Sebbene il risarcimento sia posto a carico del Titolare, questi può esercitare un'azione di rivalsa nei confronti dell'autore del danno, secondo i termini e le modalità previste dalle norme in materia di responsabilità amministrativa.

Nel caso in cui il Titolare dovesse essere assoggettato a sanzioni amministrative è previsto l'accertamento di eventuali responsabilità commesse dal personale autorizzato al trattamento di dati personali.

Per le sanzioni conseguenti a illeciti penali si rinvia all'art. 167 del Codice.

È fatta salva in ogni caso le responsabilità disciplinare eventualmente emergente dalla condotta che ha determinato l'assoggettamento a risarcimento o a sanzione.

CLAUSOLA DI REVISIONE

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