ISTITUTO NAZIONALE DI FISICA NUCLEARE

CONSIGLIO DIRETTIVO

DELIBERAZIONE n. 17603

Oggetto: Approvazione revisione del Disciplinare per l'uso delle risorse informatiche dell'INFN

Il Consiglio Direttivo dell'Istituto Nazionale di Fisica Nucleare, riunito in Roma in data 19/12/2025 alla presenza di n. 34 suoi componenti su un totale di n. 34

Visto

- Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.4.2016 (di seguito anche Regolamento) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- la propria deliberazione n. 14026 del 31 marzo 2016 con la quale è stato approvato il Disciplinare per l'uso delle risorse informatiche dell'INFN, successivamente aggiornato con deliberazione n. 15442 del 28 febbraio 2020;
- il Decreto Legislativo 30.6.2003, n. 196 e s.m.i. recante il "Codice in materia di protezione dei dati personali";
- la deliberazione di questo Consiglio n. 14844 del 27 luglio 2018 che ha definito l'organizzazione del trattamento dei dati personali all'interno dell'INFN;
- il Decreto Legislativo 7.3.2005, n. 82 e s.m.i. recante il "Codice dell'amministrazione digitale";
- la revisione del Codice di Comportamento dell'INFN, approvato con Deliberazione di questo Consiglio n. 17273 del 20.12.2024;
- il Decreto Legislativo 14.9.2015, n. 151 che ha modificato l'art. 4 della Legge 20.5.1970, n. 300, in tema di tutela della libertà e dignità dei lavoratori nei luoghi di lavoro;
- le circolari n. 1/2017 e n. 2/2017 con le quali l'Agenzia per l'Italia Digitale ha individuato le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" sulla base della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015;
- il "Regolamento per le Infrastrutture Digitali ed i Servizi Cloud per la Pubblica Amministrazione" adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024;
- il decreto legislativo 4 settembre 2024, n. 138 (decreto NIS) con cui l'Italia ha recepito la direttiva (UE) 2022/2555, relativa a "misure per un livello comune elevato di cibersicurezza nell'Unione";
- la determinazione ACN 164179 del 14 aprile 2025 e suoi allegati, recante le "Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS";
- l'articolo 12, comma 4, lettera i) dello Statuto dell'Istituto Nazionale di Fisica Nucleare in materia di attribuzioni del Consiglio Direttivo;

Considerato

- necessario l'aggiornamento del Disciplinare in relazione all'evoluzione della tecnologia e della normativa di settore e tenuto conto delle esperienze applicative maturate dalla sua entrata in vigore;
- prioritario incrementare l'efficienza e la sicurezza delle risorse di calcolo e servizi di rete, nonché la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati prodotti, raccolti o comunque trattati nell'INFN;

- le proposte di modifica al Disciplinare per l'uso delle risorse informatiche elaborate dal Gruppo di lavoro Harmony, dalla Commissione Calcolo e Reti, dal C3SN e dal RTD;

- che la Commissione Calcolo e Reti ha espresso parere favorevole in data 26 ottobre 2025, alle modifiche proposte;
- che è stato sentito il DPO dell'INFN;
- che l'esecuzione della presente deliberazione non comporta oneri aggiuntivi di bilancio.

Ritenuto

- opportuno approvare le modifiche proposte;
- necessario individuare un termine congruo per l'entrata in vigore delle modifiche.

Acquisito

- il parere della Giunta Esecutiva.

Tutto ciò premesso, con voti unanimi favorevoli

Con n. 34 voti favorevoli

DELIBERA

1. di approvare le modifiche al Disciplinare per l'uso delle risorse informatiche dell'INFN, come indicate nella tabella allegata, parte integrante alla presente deliberazione, e dei riferiti documenti accessori allegati;
2. di fissare al 19 gennaio 2026 la data di entrata in vigore delle modifiche di cui al precedente capoverso.

Titolario	**Approvazione revisione del Disciplinare per l'uso delle risorse informatiche dell'INFN**		
Data GE		**Data CD**	
Componente di Giunta competente	**D. Bettoni**		
Persona Referente			
Struttura Proponenente	**CCR**		
Direzione AC che ha curato l'istruttoria	**DSI**		
Tipologia di Atto (breve descrizione)	Nuova versione del disciplinare per l'uso delle rosorse informatiche dell'INFN per adeguamento alla evoluzione delle normative, delle infrastrutture dell'Ente, dei servizi esterni utilizzati.		
costo complessivo	0,00		
copertura finanziaria anno	**progetto**	**capitolo di spesa**	**importo**
Allegato 1	CCR_SEC_01_passowrd_policy		
Allegato 2	CCR_SEC_02_formazione_sicurezza_informatica		
Allegato 3	CCR_SEC_03_servizi_esterni		
Allegato 4	CCR_SEC_04_dispositivi_mobili		
Allegato 5	CCR_SEC_05_policy_crittografia		
Allegato 6	Norme d'uso per sistemi Linux		
Allegato 7	Norme d'uso per sistemi macOS		
Allegato 8	Norme d'uso per sistemi Windows 2.0		
Note o riferimenti Atti precedenti	Delibera CD n. 15442 del 28/02/2020 - approvazione modifiche al Disciplinare per l'uso delle risorse informatiche dell'INFN		

Disciplinare
per l’uso delle risorse informatiche dell’INFN

20 gennaio 2020	26 ottobre 2025

1. PRINCIPI GENERALI	1. PRINCIPI GENERALI
...idem...	...idem... 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 fonda- mentale 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.	**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.

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; • software e dati acquistati, prodotti o pubblicati dall'Ente;	**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 di calcolo e ai servizi di rete dell'INFN, in relazione alle funzioni ed attività che svolge nell'ambito dell'Istituto; • **Referente di gruppo di utenti**: un soggetto che coordina gli utenti e l'uso delle risorse locali di uno o più gruppi, esperimenti o servizi, in conformità alle indicazioni del Servizio di Calcolo e Reti;	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; • ~~**Referente di gruppo di utenti**: un soggetto che coordina gli utenti e l'uso delle risorse locali di uno o più gruppi, esperimenti o servizi, in conformità alle indicazioni del Servizio di Calcolo e Reti;~~ • **Utente privilegiato**: ogni soggetto che abbia credenziali di

	amministratore della risorsa individuale assegnata, senza essere nominato amministratore di sistema;
• **Amministratore di sistema**: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza;	• **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;
• **Servizio di calcolo e reti**: il servizio cui compete la gestione delle risorse di calcolo centrali, i collegamenti in rete all'interno ed all'esterno di ciascuna Struttura, nonché la cura, installazione e sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa di calcolo comunque afferente alla propria Struttura	• ~~**Servizio di calcolo e reti**~~ **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 Struttura**: il soggetto al quale, nel rispetto degli indirizzi approvati dal Consiglio Direttivo, compete la responsabilità di assicurare il funzionamento scientifico, organizzativo ed amministrativo di ciascuna Struttura come individuate nelle norme dello Statuto INFN.	• **Direttore di ~~struttura~~ 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 di calcolo e ai servizi di rete dell'INFN è consentito, previa identificazione, ai dipendenti e agli associati, nonché a collaboratori, ospiti, dottorandi, specializzandi, assegnisti,	**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 o altri autorizzati secondo le norme del presente Disciplinare.	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, eventuali ulteriori AUP e ToU specifici del servizio nonché al superamento di un corso di sicurezza informatica di livello adeguato alla criticità delle risorse. 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 è rilasciata dal Direttore di Struttura o da un suo delegato per un periodo temporale limitato alla durata del rapporto sulla base del quale è consentita l'attività all'interno dell'INFN. L'accesso è personale, non può essere condiviso o ceduto e il relativo utilizzo è consentito a ciascun utente soltanto in conformità alle norme del presente Disciplinare.	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 ~~e il relativo utilizzo è consentito a ciascun utente soltanto in conformità alle norme del presente Disciplinare~~.
5. DISPOSIZIONI GENERALI PER L'USO DELLE RISORSE INFORMATICHE ...	**5. DISPOSIZIONI GENERALI PER L'USO DELLE RISORSE INFORMATICHE** ...

Sono pertanto vietate: 1. attività contrarie alla legge nazionale, comunitaria e internazionale o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti; 2. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (spamming) o l'uso delle proprie risorse da parte di terzi per tali attività; 3. attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza e/o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, la religione, le opinioni politiche o la condizione personale o sociale; 4. attività comunque non conformi ai fini istituzionali dell'Ente. L'utilizzo delle risorse informatiche per finalità personali è tollerato purché non violi le leggi applicabili e sia compatibile con le norme del presente Disciplinare e di tutte le indicazioni stabilite dall'INFN.	Sono pertanto vietate: 1. attività contrarie alla legge nazionale, comunitaria e internazionale ~~o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti~~; 2. attività 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 e sia limitato in durata e frequenza

6. DISPOSIZIONI SPECIFICHE PER L'USO DELLE RISORSE INFORMATICHE	**6. DISPOSIZIONI SPECIFICHE PER L'USO DELLE RISORSE INFORMATICHE**
...	...
Gli Utenti inoltre:	Gli Utenti inoltre:
1. sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio di Calcolo e Reti in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'INFN in materia e pubblicate nelle pagine web del DPO INFN e dei Servizi Calcolo e Reti delle Strutture.	1. sono tenuti ad agire ~~in conformità alla legge~~ e 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.
2. nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del Servizio di Calcolo e Reti, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;	~~2. nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del Servizio di Calcolo e Reti, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;~~
3. sono responsabili dei dati e del software che installano sui computer loro affidati: procedono ad una loro attenta valutazione preliminare e non installano software privi delle regolari licenze;	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;
4. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso;	3. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati o memorizzati nei sistemi cui hanno accesso;
5. valutano attentamente l'affidabilità dei servizi esterni eventualmente utilizzati, ivi inclusi quelli di tipo cloud, in termini di sicurezza, conservazione e confidenzialità dei dati;	~~4. valutano attentamente l'affidabilità dei servizi esterni eventualmente utilizzati, ivi inclusi quelli di tipo cloud, in termini di sicurezza, conservazione e confidenzialità dei dati;~~
6. sono tenuti a seguire le indicazioni del Servizio di Calcolo e Reti per il	4. sono tenuti a proteggere il proprio account mediante password che rispettino le relative norme di

salvataggio periodico dei dati e programmi utilizzati; 7. sono tenuti a proteggere il proprio account mediante password che rispettino le norme di sicurezza indicate dall'Ente e dal Servizio Calcolo e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema; 8. non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account; 9. sono tenuti a segnalare immediatamente al proprio Referente e al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza; 10. per i sistemi operativi che lo prevedono, devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili utilizzati; 11. non devono mantenere connessioni remote inutilizzate né abbandonare la postazione di lavoro con connessioni aperte non protette. 12. sono tenuti, al termine del rapporto di lavoro/collaborazione con l'INFN a trasferire al proprio responsabile, o al Direttore di Struttura o al soggetto da questo delegato, i file di contenuto inerente l'attività di servizio/collaborazione e a cancellare in via definitiva eventuali altri file. Entro il termine di due mesi dalla cessazione del rapporto, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche	sicurezza; 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; ~~Entro il termine di due mesi dalla cessazione del rapporto, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente secondo le modalità indicate nel provvedimento~~

riferibili all'utente secondo le modalità indicate nel provvedimento del Garante per la tutela dei dati personali del 13 ottobre 2008. In caso di impossibilità o impedimento dell'Utente, ovvero laddove lo stesso, prima della cessazione del rapporto, non abbia reso disponibili i file attinenti l'attività di servizio/collaborazione e non abbia delegato un collega a inoltrarli, il Direttore, o un suo delegato, può accedere alle risorse assegnategli per il periodo necessario a recuperare i dati di interesse. In caso di grave improvvisa indisponibilità o decesso dell'Utente, il Direttore, su richiesta, potrà rendere disponibile agli aventi diritto i file con contenuti personali.	~~del Garante per la tutela dei dati personali del 13 ottobre 2008. In caso di impossibilità o impedimento dell'Utente, ovvero laddove lo stesso, prima della cessazione del rapporto, non abbia reso disponibili i file attinenti l'attività di servizio/collaborazione e non abbia delegato un collega a inoltrarli, il Direttore, o un suo delegato, può accedere alle risorse assegnategli per il periodo necessario a recuperare i dati di interesse. In caso di grave improvvisa indisponibilità o decesso dell'Utente, il Direttore, su richiesta, potrà rendere disponibile agli aventi diritto i file con contenuti personali.~~ 13. devono rispettare ogni altra indicazione in materia che dovesse essere fornita dall'Ente.
	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 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.
7. INDIVIDUAZIONE E COMPITI DEL REFERENTE DI GRUPPO DI UTENTI	~~**7. INDIVIDUAZIONE E COMPITI DEL REFERENTE DI GRUPPO DI UTENTI**~~

Il Referente del gruppo di utenti è individuato dal Direttore della Struttura cui afferisce in ragione delle funzioni assegnate. Il Referente può essere altresì individuato dalla collaborazione scientifica cui appartiene. La designazione è comunicata al Servizio di Calcolo e Reti competente. Il Referente: 1. divulga, nell'ambito del proprio gruppo, le indicazioni del Servizio di Calcolo e Reti relative alla sicurezza delle risorse ed al corretto uso delle stesse; 2. in caso di necessità, fornisce al Servizio di Calcolo e Reti informazioni o accesso alle risorse di calcolo del proprio gruppo.	~~Il Referente del gruppo di utenti è individuato dal Direttore della Struttura cui afferisce in ragione delle funzioni assegnate. Il Referente può essere altresì individuato dalla collaborazione scientifica cui appartiene. La designazione è comunicata al Servizio di Calcolo e Reti competente.~~ ~~Il Referente:~~ ~~1. divulga, nell'ambito del proprio gruppo, le indicazioni del Servizio di Calcolo e Reti~~ ~~relative alla sicurezza delle risorse ed al corretto uso delle stesse;~~ ~~2. in caso di necessità, fornisce al Servizio di Calcolo e Reti informazioni o accesso alle risorse di calcolo del proprio gruppo.~~
8. Individuazione e compiti dell'Amministratore di sistema Gli Amministratori di Sistema sono designati dal Direttore della Struttura di afferenza con apposito atto. Nel caso in cui l'attività dell'Amministratore di Sistema riguardi risorse informatiche collocate presso più Strutture, l'atto di designazione è comunicato al Direttore e al Servizio di Calcolo e Reti di ciascuna Struttura. Gli Amministratori di sistema, oltre all'osservanza di tutte le disposizioni precedenti, sono tenuti a: 1. mantenere i sistemi al livello di sicurezza appropriato al loro uso; 2. verificare con regolarità l'integrità dei sistemi; 3. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;	**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. ~~Nel caso in cui l'attività dell'Amministratore di Sistema riguardi risorse informatiche collocate presso più Strutture, l'atto di designazione è comunicato al Direttore e al Servizio di Calcolo e Reti di ciascuna Struttura~~ Gli amministratori di sistema, oltre 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;
4. segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione; 5. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono; 6. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi; 7. in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati; 8. seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.	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 ~~e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi~~; 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.
9. Compiti del servizio calcolo e reti Il Servizio Calcolo e Reti, al fine di mantenere il più elevato livello di	**6.4. Team responsabile delle risorse informatiche** Il team responsabile delle risorse

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

7. fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti.	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**.
10. Disposizioni per l'uso dei servizi esterni Il trattamento dei dati personali di qualunque tipo o di particolare rilevanza per l'Ente può essere effettuato mediante l'uso di servizi esterni, anche di tipo cloud, soltanto ove l'INFN abbia preventivamente verificato i rischi e i benefici connessi ai servizi offerti, i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati oltre ai profili di responsabilità nel trattamento.	**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 è mantenuto aggiornato dalla Commissione Calcolo e Reti.
11. TRATTAMENTO DEI DATI ACQUISITI IN RELAZIONE ALL'USO DELLE RISORSE DI CALCOLO E ALL'ACCESSO AI SERVIZI DI RETE L'INFN, nel rispetto dei principi di libertà e dignità, non consente l'installazione di strumentazioni hardware e software mirate al controllo degli utenti e vieta il trattamento effettuato mediante apparecchiature preordinate al controllo a distanza quali: la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio di posta elettronica; b) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente; c) la lettura e registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi; d) l'analisi occulta di computer portatili affidati in uso. Con riferimento all'accesso alla rete, il Servizio Calcolo e Reti, per le finalità indicate al punto 14eriod14ive raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente; non registra il contenuto delle connessioni, può raccogliere tuttavia alcune informazioni relative alle	~~**11. TRATTAMENTO DEI DATI ACQUISITI IN RELAZIONE ALL'USO DELLE RISORSE DI CALCOLO E ALL'ACCESSO AI SERVIZI DI RETE**~~ ~~L'INFN, nel rispetto dei principi di libertà e dignità, non consente l'installazione di strumentazioni hardware e software mirate al controllo degli utenti e vieta il trattamento~~ ~~effettuato mediante apparecchiature preordinate al controllo a distanza quali:~~ ~~la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio di posta elettronica;~~ ~~b) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;~~ ~~c) la lettura e registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi;~~ ~~d) l'analisi occulta di computer portatili affidati in uso.~~ ~~Con riferimento all'accesso alla rete, il Servizio Calcolo e Reti, per le finalità indicate al punto 14eriod14ive raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente; non registra il contenuto delle connessioni, può raccogliere tuttavia alcune informazioni relative alle~~

transazioni eseguite quali: indirizzi dei nodi, ora di inizio e fine transazione e quantità dei dati trasferiti. I dati di cui al paragrafo precedente sono conservati per un 15eriod non superiore a un anno e sono utilizzabili dal personale del Servizio di Calcolo e Reti competente solamente con fini di controllo della sicurezza e per l'ottimizzazione dei sistemi. Le Strutture in cui sono installati proxy server o altri sistemi di controllo delle sessioni possono conservare i file di log contenenti informazioni relative alle pagine web, interne o esterne, accedute dai nodi locali. Tali informazioni, conservate per un 15eriod non superiore a sette giorni a cura del Servizio di Calcolo e Reti, sono esaminate o elaborate soltanto ove si ravvisi la necessità di garantire la sicurezza o il buon funzionamento del sistema.	~~transazioni eseguite quali: indirizzi dei nodi, ora di inizio e fine transazione e quantità dei dati trasferiti. I dati di cui al paragrafo precedente sono conservati per un 15eriod non superiore a un anno e sono utilizzabili dal personale del Servizio di Calcolo e Reti competente solamente con fini di controllo della sicurezza e per l'ottimizzazione dei sistemi. Le Strutture in cui sono installati proxy server o altri sistemi di controllo delle sessioni possono conservare i file di log contenenti informazioni relative alle pagine web, interne o esterne, accedute dai nodi locali. Tali informazioni, conservate per un 15eriod non superiore a sette giorni a cura del Servizio di Calcolo e Reti, sono esaminate o elaborate soltanto ove si ravvisi la necessità di garantire la sicurezza o il buon funzionamento del sistema.~~
12. RACCOLTA DATI IN RELAZIONE AL SERVIZIO DI POSTA ELETTRONICA Il Servizio di Calcolo e Reti per esigenze organizzative connesse al funzionamento, sicurezza e salvaguardia del servizio di posta elettronica registra data, ora, indirizzi del mittente e del destinatario dei messaggi di posta, nonché il risultato delle analisi dei software antivirus ed antispam. I dati registrati, utilizzati anche per elaborazioni statistiche, sono conservati per un period non superiore a un anno e sono accessibili dal solo personale, appositamente incaricato, del Servizio di Calcolo e Reti di competenza. Per le medesime finalità le Strutture che effettuano copie di salvataggio dei messaggi di posta elettronica conservano tali copie per un periodo non	~~**12. RACCOLTA DATI IN RELAZIONE AL SERVIZIO DI POSTA ELETTRONICA**~~ ~~Il Servizio di Calcolo e Reti per esigenze organizzative connesse al funzionamento, sicurezza e salvaguardia del servizio di posta elettronica registra data, ora, indirizzi del mittente e del destinatario dei messaggi di posta, nonché il risultato delle analisi dei software antivirus ed antispam. I dati registrati, utilizzati anche per elaborazioni statistiche, sono conservati per un period non superiore a un anno e sono accessibili dal solo personale, appositamente incaricato, del Servizio di Calcolo e Reti di competenza. Per le medesime finalità le Strutture che effettuano copie di salvataggio dei messaggi di posta elettronica conservano tali copie per un periodo non~~

superiore a un anno a cura del Servizio di Calcolo e Reti di competenza. Ciascuna Struttura, ove compatibile con la propria organizzazione, può rendere disponibili indirizzi di posta elettronica condivisi attraverso l'uso di liste di distribuzione di e-mail, nonché messaggi di risposta automatica, in caso di assenza programmata dei titolari. La casella di posta elettronica è disattivata entro i due mesi successivi alla scadenza del termine nel quale l'utente è stato autorizzato all'accesso. Entro tale periodo l'utente ha il dovere di trasferire al Direttore o a un suo delegato le comunicazioni di servizio d'interesse e di trasmettergli quelle nel frattempo intervenute. Il contenuto della casella è comunque cancellato entro un anno dalla scadenza del termine di autorizzazione all'accesso. I periodi indicati nel presente capoverso possono essere prolungati dal Direttore ove ne ravvisi specifica esigenza. In caso di impossibilità o impedimento del titolare della casella di posta elettronica, il Direttore o un suo delegato può avere accesso alla casella per un periodo non superiore a un mese dalla data di conoscenza della situazione che ha determinato l'impossibilità o l'impedimento.	~~superiore a un anno a cura del Servizio di Calcolo e Reti di competenza.~~ ~~Ciascuna Struttura, ove compatibile con la propria organizzazione, può rendere disponibili indirizzi di posta elettronica condivisi attraverso l'uso di liste di distribuzione di e-mail, nonché messaggi di risposta automatica, in caso di assenza programmata dei titolari.~~ ~~La casella di posta elettronica è disattivata entro i due mesi successivi alla scadenza del termine nel quale l'utente è stato autorizzato all'accesso. Entro tale periodo l'utente ha il dovere di trasferire al Direttore o a un suo delegato le comunicazioni di servizio d'interesse e di trasmettergli quelle nel frattempo intervenute. Il contenuto della casella è comunque cancellato entro un anno dalla scadenza del termine di autorizzazione all'accesso. I periodi indicati nel presente capoverso possono essere prolungati dal Direttore ove ne ravvisi specifica esigenza.~~ ~~In caso di impossibilità o impedimento del titolare della casella di posta elettronica, il~~ ~~Direttore o un suo delegato può avere accesso alla casella per un periodo non superiore a un mese dalla data di conoscenza della situazione che ha determinato l'impossibilità o l'impedimento.~~
	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. 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. **9.7 Accesso urgente ed improrogabile ad informazioni di servizio** Qualora fosse necessario ed improrogabile accedere a dati o messaggi inerenti all'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[1].

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

13. Ulteriori misure per la tutela dei sistemi informativi	**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 adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine il Servizio di Calcolo e Reti può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.	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, nonostante l'adozione di accorgimenti tecnici preventivi, si verifichino eventi dannosi o rilevino comportamenti anomali o non consentiti, il Servizio di Calcolo e Reti esegue, previa informazione agli interessati e salvo i casi di necessità ed urgenza, ulteriori accertamenti e adotta le misure necessarie ad interrompere le condotte dannose o non consentite.	Nel caso in cui si verifichino eventi dannosi o si rilevino comportamenti non consentiti, il team 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 e già segnalati o di particolare gravità, il Responsabile del Servizio di Calcolo e Reti adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al Direttore di Struttura, che dispone gli ulteriori provvedimenti ai sensi del punto seguente.	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**”.
I Direttori di Struttura, in relazione alle funzioni loro assegnate circa il trattamento dei dati personali, adottano ogni opportuna misura affinché i soggetti preposti al trattamento dei dati relativi all'uso di internet e della posta elettronica svolgano soltanto le operazioni strettamente necessarie al perseguimento delle relative finalità,	~~I Direttori di Struttura, in relazione alle funzioni loro assegnate circa il trattamento dei dati personali, adottano ogni opportuna misura affinché i soggetti preposti al trattamento dei dati relativi all'uso di internet e della posta elettronica svolgano soltanto le operazioni strettamente necessarie al perseguimento delle relative finalità,~~

senza realizzare attività di controllo a distanza, neppure di propria iniziativa.	~~senza realizzare attività di controllo a distanza, neppure di propria iniziativa.~~
15. Informativa Il presente Disciplinare costituisce informativa ai sensi dell'art. 4, c. 3, della legge 20 maggio1970 n.300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse di calcolo e dei servizi di rete. L'INFN assicura al presente Disciplinare e ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti mediante pubblicazione nella pagina web di ciascuna Struttura, nonché consegnandolo a ciascuno in modalità elettroniche o cartacee, idonee comunque a dimostrare l'avvenuta consegna. Il presente Disciplinare abroga e sostituisce integralmente tutti i precedenti regolamenti adottati in materia.	**13. Disposizoni finali.** ~~Il presente Disciplinare costituisce informativa ai sensi dell'art. 4, c. 3, della legge 20 maggio1970 n.300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse di calcolo e dei servizi di rete.~~ 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.
16. CLAUSOLA DI REVISIONE Il presente Disciplinare è aggiornato periodicamente in relazione all'evoluzione della tecnologia e della normativa di settore.	**14. CLAUSOLA DI REVISIONE** .. idem ...

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.

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 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 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**

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.