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).