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