

Norme d'uso per sistemi operativi Windows

v 2.0 – 01/10/2025

Sommario

Introduzione.....	3
Responsabilità dell'amministratore di sistema.....	4
Installazione e configurazione del sistema operativo	4
Installazione.....	5
Configurazione e primo avvio	6
Versione del sistema operativo.....	6
Nome del computer	6
Nome utente	6
Impostare la verifica delle signature dei pacchetti	6
Rimozione dei pacchetti non necessari.....	6
Creare vincoli sulle password.....	6
Blocco di account speciali	7
Accesso a servizi da parte di utenti specifici	7
Accesso a porte o servizi specifici tramite rete	7
Condivisione di file	7
Accesso remoto al sistema.....	7
Manutenzione	8
Aggiornamento del sistema	8
Verifica degli account e delle credenziali	8
Gestione degli utenti.....	8
Gestione di file con dati critici o "rilevanti" per l'ente	9
Difese contro i malware.....	10
Copie di sicurezza.....	11
Protezione dei dati tramite crittografia	11
Compromissione del sistema	11
File di log.....	12

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 delle 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** essere 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 essere 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 rimovibili (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 sicurezza¹.

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 installazione².

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**