Norme d'uso
per sistemi operativi Windows

Allegato A3

v 1.2

Attuazione della Circolare AgID 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

Livello Minimo

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, per dispositivi che utilizzano sistema operativo Windows **limitatamente al solo livello minimo di sicurezza** richiesto nella circolare, cioè al livello sotto il quale nessuna amministrazione pubblica può scendere.

Le indicazioni riportate di seguito mirano a soddisfare gli obblighi espressi dalla circolare AgID ma non sostituiscono, piuttosto integrano, quanto già riportato nei documenti delle “Linee guida sulla sicurezza informatica” della Commissione Calcolo e Reti:

- Norme generali per l'accesso e l'uso delle risorse informatiche dell'INFN (C.D. 23/02/2007);
- Carta della Sicurezza Informatica (C.D. 23/02/2007);
- Windows base (20/12/2005);
- Windows avanzato (20/12/2005);
- Servizi centralizzati (20/12/2005);
- Gestione incidenti (20/12/2005);
- Sicurezza della LAN (19/12/2005);

consultabili alle URL

- https://web.infn.it/CCR/index.php/it/sito-utenti-del-calcolo/sicurezza-informatica,
- https://web.infn.it/CCR/index.php/it/sito-utenti-del-calcolo/sicurezza-informatica/56-progetti-dei-gruppi-di-lavoro/documentazione-progetti/81-documenti-progetto-harmony

Questa guida risulta un aggiornamento ed un ampliamento dei documenti “Windows base (20/12/2005)” “Windows avanzato (20/12/2005)” e alla luce di quanto richiesto dalla circolare ed è rivolta agli utenti che sono in possesso delle credenziali di accesso come amministratori di sistema.

Quanto richiesto dalla circolare limitatamente al solo livello minimo di sicurezza è riportato in **Appendice A**.

Ogni singola misura di sicurezza verrà citata tramite il relativo numero identificativo ABSC ID (Agid Basic Security Control(s) Id Number).

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 immagini virtuali o preconfigurazioni, le credenziali di amministrazione DEVONO essere modificate prima di collegare il sistema alla rete [ABSC ID 5.3.1].

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.*

Installazione

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

Se l'immagine di installazione non è stata fornita dal Servizio Calcolo, **DEVE** essere salvata su supporti conservati *offline* [ABSC ID 3.3.1].

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 [ABSC ID 2.1.1].

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 Servizio Calcolo e Reti.

In ogni caso **NON SI DEVONO** utilizzare indirizzi IP arbitrari non assegnati dai Servizi Calcolo e Reti (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.

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):

- abbiano un'elevata robustezza [ABSC ID 5.7.1],
- vengano sostituite con sufficiente frequenza [ABSC ID 5.7.3],
- non vengano riutilizzate a breve distanza di tempo [ABSC ID 5.7.4].

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`**)

Per le macchine in Dominio Active Directoy si suggerisce di assegnare all'account locale con i privilegi di amministratore una password casuale. Per accedere alla macchina come utente con i privilegi di amministratore verranno utilizzati gli account di dominio privilegiati creati per ogni amministratore.

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

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), specificando opportunamente gli account che potranno eseguirlo [ABSC ID 3.4.1].

Primo backup

Completata la procedura di installazione e configurazione **SI DEVE** eseguire un backup completo del sistema da poter essere utilizzato per ripristinare il sistema in caso di compromissioni [ABSC ID 3.2.2]. Tale backup **DEVE** essere memorizzato *offline* [ABSC ID 3.3.1], per esempio, su CD o DVD.

A tal fine si possono utilizzare software specifici come, ad esempio, *clonezilla*.

Per gli utenti di Dominio Active Directory si consiglia di abilitare il profilo **roaming**.

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 [ABSC ID 4.8.2]. Si suggerisce di abilitare gli aggiornamenti automatici sia per il sistema operativo sia per il software installato [ABSC ID 4.5.1].

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 [ABSC ID 4.8.2].

Qualora non sia possibile risolvere le vulnerabilità accertate **SI DEVE** documentare il rischio accettato [ABSC ID 4.7.1], dandone anche comunicazione al Servizio Calcolo e Reti.

A seguito di modifiche significative del sistema (p.e. aggiunta di nuovi servizi), **È OBBLIGATORIO** concordare con il Servizio Calcolo l'esecuzione di una scansione di sicurezza per individuare eventuali ulteriori vulnerabilità [ABSC ID 4.1.1]. A scansione avvenuta, **DEVONO** essere intraprese tutte le azioni necessarie per risolvere le vulnerabilità accertate o, qualora non sia possibile, documentare il rischio accettato [ABSC ID 4.7.1], dandone anche comunicazione al Servizio Calcolo.

Verifica degli account e delle credenziali

Al fine di verificare la robustezza delle credenziali amministrative impostare le opportune *group policy* (lunghezza minima, complessità) ed eseguire periodicamente controlli con programmi specifici sui file di password degli account utente. [ABSC ID 3.1.1, 3.2.1, 5.7.1].

Gestione degli utenti

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 [ABSC ID 5.5.1].

DEVE essere mantenuto l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata [ABSC ID 5.2.1].

Le utenze amministrative **DEVONO** essere utilizzate solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato [ABSC ID 5.1.2].

DEVE essere assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse [ABSC ID 5.10.1]. 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 [ABSC ID 5.10.2].

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'antivirus messo a disposizione dall'ente [ABSC ID 8.1.1] impostando l'aggiornamento automatico e l'esecuzione automatica delle scansioni anti-malware dei supporti rimovibili al momento della loro connessione [ABSC ID 8.8.1].

È OBBLIGATORIO l'uso di un firewall personale e le funzionalità IPS dell'antivirus **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 [ABSC ID 8.3.1].

È OBBLIGATORIO disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili [ABSC ID 8.7.1].

È OBBLIGATORIO disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file [ABSC ID 8.7.2].

È OBBLIGATORIO disattivare l'apertura automatica dei messaggi di posta elettronica [ABSC ID 8.7.3].

È OBBLIGATORIO disattivare l'anteprima automatica dei contenuti dei file [ABSC ID 8.7.4].

Copie di sicurezza

È OBBLIGATORIO effettuare almeno settimanalmente una copia di sicurezza delle “informazioni strettamente necessarie per il completo ripristino del sistema” [ABSC ID 10.1.1].

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 [ABSC ID 10.3.1], 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 [ABSC ID 10.4.1][1].

Protezione dei dati tramite crittografia

Per i portatili si consiglia l'uso di un *filesystem* criptato 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 [ABSC ID: 13.1.1].

Compromissione del sistema

In caso di compromissione del sistema informare immediatamente il Servizio Calcolo e Reti 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[2] o come una nuova installazione[3] [ABSC ID 3.2.2].

1 La richiesta è volta a migliorare la protezione contro ransomware (Reveton, CryptoLocker, WannaCry, …).
2 Vedi “Primo backup”.
3 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**

APPENDICI

Appendice A - Circolare AgID 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) - Livello Minimo

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC ID	Descrizione
1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC ID	Descrizione
2.1.1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC ID	Descrizione
3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3.3.1	Le immagini d'installazione devono essere memorizzate offline.
3.4.1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC ID	Descrizione
4.1.1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
4.7.1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4.8.1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
4.8.2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC ID	Descrizione
5.1.1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5.10.3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC ID	Descrizione
8.1.1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.
8.3.1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file.
8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
8.9.2	Filtrare il contenuto del traffico web.
8.9.3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC ID	Descrizione
10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
10.3.1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
10.4.1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC ID	Descrizione
13.1.1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist.