Norme d'uso
per sistemi operativi Apple macOS

V 1.3

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, nel seguito chiamata **Circolare**, per dispositivi che utilizzano sistema operativo Apple macOS, *limitatamente al solo livello minimo di sicurezza* in essa richiesto, cioè al **livello sotto il quale nessuna amministrazione pubblica può scendere**.

Le indicazioni di seguito mirano a soddisfare gli obblighi espressi dalla Circolare e 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);
- 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 deriva dal documento *Norme d’uso per sistemi operativi GNU/LINUX* alla luce di quanto richiesto dalla Circolare ed è rivolta agli utenti che sono in possesso delle credenziali di amministratore 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,

SI DEVE / SI DEVONO.

Sarà compito e responsabilità dell'amministratore del sistema attuare quanto indicato.

Tutto ciò che non viene identificato tramite tali parole chiave rappresenta un mero suggerimento non previsto esplicitamente nel livello minimo di sicurezza della Circolare, ma comunque consigliato 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] si consiglia di coordinare con il Servizio di Calcolo della propria Struttura la fase di installazione e configurazione di sistemi operativi macOS, secondo le modalità stabilite dal Servizio stesso, oltre a quelle riportate in questa guida.

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)

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 Apple attraverso le procedure standard di Recovery o direttamente fornite dal Servizio Calcolo.

Nel caso si utilizzino immagini virtuali, *container* o *docker* preconfezionati, le credenziali di amministrazione **DEVONO** essere modificate prima del collegamento alla rete [ABSC ID 5.3.1][2].

Se l'immagine di installazione non è stata fornita dal Servizio Calcolo, **DEVE** essere salvata *offline*.

Nei limiti del possibile, installare solo versioni supportate e stabili, evitando di usare versioni obsolete e non piu' supportate da Apple.

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 [ABSC ID 2.1.1].

In accordo con quanto indicato nel *Disciplinare per l'uso delle risorse informatiche*, gli indirizzi IP utilizzati **DEVONO** essere assegnati dal Servizio Calcolo (direttamente o tramite server DHCP).

Configurazione e primo avvio

Le password di tutte le utenze amministrative:

- **DEVONO** essere di robustezza elevata [ABSC ID 5.7.1].
- **DEVONO** essere modificate con sufficiente frequenza (*password aging*) [ABSC ID 5.7.3].
- **NON DEVONO** essere riutilizzate a breve distanza di tempo (*password history*) [ABSC ID 5.7.4].

2 Per esempio disabilitando l'interfaccia di rete e collegandosi come amministratore alla console virtuale.

Ogni forma di login come **`root`**, incluso l'accesso via **ssh**, **DEVE** essere disabilitata [ABSC ID 5.10.3]

Per accedere da remoto al sistema **SI DEVE** impiegare solo software che utilizzi protocolli sicuri (per es. *ssh*, *scp*, ...) [ABSC ID 3.4.1]

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`

Accesso remoto al sistema

Per accedere da remoto al sistema **SI DEVE** impiegare solo software che utilizza protocolli sicuri (per es. **ssh**, **scp**, ...) [ABSC ID 3.4.1].

Prima copia di sicurezza

Una volta completata la procedura di installazione e configurazione **DEVE** essere eseguito un backup completo del sistema, da utilizzare per un ripristino in caso di compromissioni [ABSC ID 3.2.2]. Tale backup **DEVE** essere conservato offline [ABSC ID 3.3.1], p.e. su CD o DVD.

A tal fine si possono utilizzare software generici come *clonezilla* oppure i tool standard forniti da Apple come *DiskUtility* e/o il comando *asr.*

Manutenzione

Aggiornamento del sistema

Il sistema **DEVE** essere mantenuto costantemente aggiornato. In particolare **SI DEVONO** applicare tutte le patch di sicurezza appena disponibili [ABSC ID 4.8.2]. 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 [ABSC ID 4.5.1].

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 [ABSC ID 4.8.2].

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.

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 [ABSC ID 5.5.1].

È OBBLIGATORIO mantenere 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 solamente per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato [ABSC ID 5.1.2]. A tal fine **È OBBLIGATORIO** utilizzare sempre il comando **`sudo`** per eseguire comandi di amministrazione.

Dalla versione macOS El Capitan 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 OBBLIGATORIO assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali **DEVONO** 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 con diritti *Admin* (gruppo **`sudoers`***)* 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 [ABSC ID 5.10.2].

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.

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-- --- ---`).

Difese contro i malware

È OBBLIGATORIO installare l'antivirus (*antimalware*) messo a disposizione dall'ente [ABSC ID 8.1.1] impostando l'aggiornamento automatico e la scansione dei supporti rimovibili al momento della loro connessione [ABSC ID 8.8.1 e 8.8.1].

È OBBLIGATORIO abilitare il *firewall* [ABSC ID 8.1.2].

È OBBLIGATORIO limitare l'uso di dispositivi esterni 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 rimovibili [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* **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione [ABSC ID 10.3.1], assicurandosi che il backup non sia accessibile via rete in modo permanente onde evitare che eventuali attacchi possano coinvolgere anche tutte le sue copie di sicurezza [ABSC ID 10.4.1][3].

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 [ABSC ID: 13.1.1][4].

3 La richiesta è volta a migliorare la protezione contro ransomware (Reveton, CryptoLocker, WannaCry, …).
4 Vedi anche la sezione “Gestione di file con dati critici o “rilevanti” per l'ente”.

Compromissione del sistema

In caso di compromissione del sistema DEVE essere immediatamente informato il Servizio Calcolo e concordata la procedura di ripristino.

Il ripristino del sistema **DEVE** essere eseguito tramite le immagini salvate a conclusione della fase di installazione e configurazione[5] o come una nuova installazione[6] [ABSC ID 3.2.2].

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.

Dove possibile, si raccomanda di mantenere una copia dei messaggi su di un'altra macchina (logging remoto).

Altre raccomandazioni

- Si consiglia di installare software per il controllo dell'integrità dei file di sistema
- Si consiglia di analizzare sistematicamente la compliance alle policy di security proposte dagli organismi di certificazione (CIS,NIST,SANS,etc)

5 Vedi "Prima copia di sicurezza".
6 Vedi "Installazione".

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.