ISTITUTO NAZIONALE DI FISICA NUCLEARE

CONSIGLIO DIRETTIVO

DELIBERAZIONE N. 14844

Il Consiglio Direttivo dell'Istituto Nazionale di Fisica Nucleare, riunitosi a Roma in data 27 luglio 2018, alla presenza di n. 32 dei propri componenti su un totale di 34,

- visto il D.Lgs. 196/2003 contenente il "*Codice in materia di protezione dei dati personali*";
- vista la Raccomandazione della Commissione europea del 11.3.2005 riguardante la Carta Europea dei ricercatori e un Codice di Condotta per l'assunzione dei ricercatori che all'Allegato 1, nel paragrafo dedicato alla "*Buona Condotta nel settore della ricerca*", afferma che i ricercatori dovrebbero essere al corrente dei vigenti requisiti legali nazionali per quanto riguarda la protezione dei dati e della riservatezza e adottare le misure necessarie per soddisfarli in qualsiasi momento;
- visto il D.Lgs. n. 218/2016 il quale all'art. 2, comma 2, lett. e) dispone che i ricercatori e i tecnologi devono assicurare la protezione e la riservatezza dei dati trattati;
- visto il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27.4.2016 (di seguito anche Regolamento) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati;
- visto l'art. 4 comma 1, punto 7) del Regolamento che definisce Titolare del trattamento l'autorità pubblica che determina le finalità e i mezzi del trattamento dei dati personali;
- visto l'art. 24 del Regolamento il quale dispone che il Titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche;
- viste le deliberazioni del Consiglio Direttivo n. 6389 del 26.3.1999 e n. 8335 del 28.11.2003 che hanno individuato il titolare nonché i responsabili del trattamento dei dati personali all'interno dell'INFN ai sensi della legge n. 675/1996, contenente norme sulla "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*";
- vista la deliberazione del Consiglio Direttivo n. 14734 del 27.4.2018 che ha designato il Responsabile della protezione dei dati personali dell'INFN (di seguito DPO);
- visto lo Statuto dell'INFN;
- visto il Regolamento di Organizzazione e Funzionamento dell'INFN;
- visto il Disciplinare Organizzativo dell'Amministrazione Centrale;
- ravvisata l'esigenza di adeguare l'organizzazione del trattamento dei dati personali all'interno dell'INFN in considerazione del Regolamento;
- ritenuto di individuare, in questa prima fase di implementazione del Regolamento all'interno dell'organizzazione dell'Istituto, delle misure tecniche di sicurezza alle quali le Strutture dell'INFN e le articolazioni dell'Amministrazione Centrale e della Presidenza devono adeguarsi
- sentito il DPO dell'INFN;
- con il voto favorevole di n. 32 componenti

DELIBERA

1. L'Istituto Nazionale di Fisica Nucleare è individuato Titolare del trattamento dei dati personali cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento.
2. Il Direttore Generale dell'INFN, sentito il DPO, svolge funzioni di coordinamento ed in particolare: fornisce indicazioni di carattere generale; emana direttive; definisce modelli standard delle informative, degli atti di designazione e delle istruzioni nonché dei contratti di designazione dei Responsabili esterni al trattamento; coordina la definizione delle misure tecniche ed organizzative volte ad assicurare all'interno dell'INFN il corretto adempimento del Regolamento e la concreta applicazione delle indicazioni provenienti dall'Autorità di controllo.
3. Il Direttore Generale, i Direttori delle Strutture, i Direttori delle Aree, Direzioni, Divisioni e Servizi Professionali dell'Amministrazione Centrale, di cui all'art. 2 del Disciplinare Organizzativo dell'Amministrazione Centrale, nonché i Responsabili del Servizio di Presidenza e dell'Ufficio Comunicazione, negli ambiti di rispettiva competenza definiti dagli atti interni dell'Istituto, assicurano il rispetto di tutti gli obblighi previsti dal Regolamento e dalla normativa nazionale in capo al Titolare del trattamento;
4. I Direttori delle Strutture dell'INFN, in considerazione dell'attuale organizzazione dei sistemi informativi, attuano le misure tecniche di sicurezza contenute nell'allegato e parte integrante alla presente deliberazione, integrandole, se del caso, per assicurare un più efficace livello di sicurezza dei dati personali all'interno della Struttura che dirigono; assicurano, su base permanente, la riservatezza, la disponibilità e la resilienza dei sistemi esistenti nella Struttura, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la predisposizione e l'esecuzione con regolarità di procedure per verificare e valutare l'efficacia delle misure adottate;
5. I soggetti individuati nel capoverso 3 hanno il compito di provvedere alla effettiva e concreta attuazione delle misure tecniche ed organizzative volte a garantire e dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento presso ciascuna Struttura, articolazione o ufficio che dirigono o di cui hanno la responsabilità. In particolare:
   a) designano le persone autorizzate al trattamento dei dati personali nell'ambito della articolazione che dirigono; garantiscono che le stesse siano state preliminarmente istruite per il trattamento e si siano impegnate alla riservatezza; verificano l'osservanza delle istruzioni che sono state impartite per il trattamento, e, ove ne sussistano le condizioni, l'osservanza di obblighi legali di riservatezza;
   b) assicurano che l'informativa sul trattamento dei dati sia fornita all'interessato e, nei casi previsti, ne acquisiscono il consenso;
   c) danno seguito alle eventuali richieste degli interessati per l'esercizio dei diritti loro garantiti dal Capo IV del Regolamento;
   d) implementano il Registro del trattamento dei dati personali, comunicando al DPO i nuovi trattamenti in uso presso la Struttura o l'articolazione che dirigono o di cui hanno la responsabilità;
   e) notificano al Garante della protezione dei dati personali le violazioni dei dati personali (*data breach*); provvedono alla comunicazione della violazione agli interessati, ai sensi degli articoli 33 e 34 del Regolamento, e ne danno informativa al Direttore Generale e al DPO;
   f) effettuano, quando sia necessaria e sentito il DPO, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali;

g) mettono a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi richiesti dal Regolamento; consentono e contribuiscono alle attività di revisione e di ispezione;
h) informano immediatamente il Direttore Generale e il DPO in ogni circostanza in cui ritengono che un'istruzione relativa al trattamento dei dati violi il Regolamento o altre disposizioni relative alla protezione dei dati;
i) designano quali Responsabili esterni al trattamento i soggetti che trattano dati personali per conto dell'INFN nell'ambito di convenzioni o contratti che hanno potere a sottoscrivere, nell'ambito delle competenze per valore e materia previste dagli atti interni dell'INFN;
j) individuano un referente locale quale punto di contatto con il DPO e supporto alle attività di gestione degli adempimenti connessi alla protezione dei dati.

6. Gli oneri derivanti dall'esecuzione della presente deliberazione trovano copertura sul bilancio delle singole Strutture nelle spese di funzionamento.

Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali nell’INFN

V 1.0
Luglio 2018

Istituto Nazionale di Fisica Nucleare

Introduzione

Questa documento riporta le norme tecniche e organizzative, relative ai sistemi in uso nell'INFN (Windows, Linux e macOS), ritenute adeguate a garantire la sicurezza dei dati personali trattati, compresa la loro protezione da trattamenti non autorizzati o illeciti e dalla loro perdita, distruzione o danno accidentale, secondo quando indicato nell'Art. 5 del Regolamento UE N. 2016/679 (Regolamento).

Al fine di proporre norme precise e non ridondanti, utili a tradursi in effettive misure di sicurezza per i sistemi interessati, è stata presa attentamente in esame la recente disciplina AgID: Circolare AgID 18/04/2017, n. 2/2017, GU Serie Generale n.103 del 05/05/2017 (Circolare), di cui si riporta in Appendice la tabella riassuntiva delle misure obbligatorie previste[1].

Allo stato attuale, si ritiene che l'attuazione di quanto richiesto nella Circolare soddisfi, almeno per la gran parte dei casi, quei requisiti di sicurezza che il Regolamento impone. Considerato però che il Regolamento non entra nello specifico delle misure da adottare, ma lascia al titolare la valutazione della congruità delle azioni intraprese, si precisa che quanto qui richiesto è da ritenersi solo un *buon punto di partenza.* L'attuazione delle presenti norme dovrà pertanto essere valutata in ciascuna Struttura ed eventualmente adattata alle particolari situazioni locali, *documentando con chiarezza* il motivo delle scelte fatte. Il DPO è sempre a disposizione per consulenze e suggerimenti in merito, raggiungibile presso dpo@infn.it.

Le norme di seguito sono principalmente rivolte agli utenti in possesso delle credenziali di amministratore di sistema. Gli utenti non privilegiati faranno riferimento all'amministratore della loro macchina per indicazioni specifiche.

Le procedure, azioni e configurazioni volte all'attuazione di quanto richiesto saranno indicate con le seguenti parole chiave e incluse in un rettangolo (nel caso di misure necessarie solo 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.

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

Tutte le indicazioni non individuate dalle parole chiave di sopra sono *suggerimenti* consigliati per migliorare la sicurezza del sistema.

Parte I
Sistemi Linux

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 GNU/Linux, secondo le modalità stabilite dal Servizio.

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`**).

Installazione

Se non si utilizza un sistema di installazione predisposto dal Servizio Calcolo, **SI DEVONO** usare solamente immagini prelevate dai *repository* ufficiali o fornite dal Servizio Calcolo, verificandone il *checksum*.

Se si impiegano 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 su supporti conservati *offline* (per esempio CD o DVD o tape library [ABSC ID 3.3.1]).

Nei limiti del possibile si raccomanda di installare solo versioni supportate e stabili, evitando di usare versioni obsolete o di test.

Nel caso di server su consiglia di effettuare un'istallazione *minimale* del sistema operativo, limitandosi al solo software strettamente necessario.

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 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** avere elevata robustezza, non essere banali o presenti nei dizionari di qualsiasi lingua [ABSC ID 5.7.1],
- **DEVONO** essere modificate con sufficiente frequenza [ABSC ID 5.7.3],
- **NON DEVONO** essere riutilizzate a breve distanza di tempo [ABSC ID 5.7.4].

Ogni forma di login come `root` al di fuori delle *virtual console* (`tty*`), incluso l'accesso via **ssh**, **DEVE** essere disabilitata [ABSC ID 5.10.3].

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

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. `bin`) 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 `iptables` o *tcp_wrapper* (file `/etc/hosts.allow` e `/etc/hosts.deny`);
- controllare l'accesso a servizi e risorse da parte di utenti specifici tramite le librerie PAM.

Condivisione di filesystem: nfs

Si tratta di un servizio intrinsecamente insicuro, poiché è basato su *UID* e *GID* dell'utente remoto. Se è necessario usarlo, si raccomanda di configurarlo correttamente impostando almeno le seguenti restrizioni:

- evitare *wildcard* in **`/etc/exports`**;
- impedire l'accesso a **`root`** (se possibile)[3];
- montare il filesystem in read-only (se possibile)[4];
- limitare sempre l'esposizione del filesystem ai soli host necessari;

3 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, ...).

4 Anche in questo caso la richiesta è inapplicabile nella quasi totalità dei casi ma valutarne comunque la possibilità per limitare i danni di eventuali ransomware.

- controllare la situazione con il comando `showmount` utilizzando le opzioni `-e` e `-a`;
- nel caso in cui il filesystem sia inserito in **`/etc/fstab`** usare l'opzione `no-suid`;
- se possibile filtrare le porte 111 e 2049 (TCP e UDP) tramite `iptables`;
- inserire il servizio *portmapper* fra quelli controllati da `iptables` o in alternativa usare **tcp_wrapper**.

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].

Per semplificare 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. Se è necessario utilizzarle si consiglia di:

- usare `iptables` o **tcp_wrappers** (file `/etc/hosts.allow` e `/etc/hosts.deny`);
- ridurre al minimo le macchine da cui si accetta il login senza autorizzazione, in ogni caso mai esterne alla LAN.

Prima copia di sicurezza

Una volta completata la procedura di installazione e configurazione, **DEVE** essere eseguito un backup completo del sistema[5], da utilizzare per un ripristino in caso di compromissioni [ABSC ID 3.2.2], che **DEVE** essere conservato offline [ABSC ID 3.3.1][6],

5 Si possono utilizzare software specifici come **clonezilla** o semplicemente **`dd`** + **`gzip`.**
6 Misura non necessaria se l'eventuale ripristino viene sempre fatto a partire dall'immagine originale.

Manutenzione

Aggiornamento del sistema

Il sistema **DEVE** essere mantenuto costantemente aggiornato. In particolare **SI DEVONO** applicare tutte le *patch* di sicurezza non appena disponibili [ABSC ID 4.8.2]. Per far questo possono essere impostati aggiornamenti automatici (p.e. tramite `cron`) sia per i pacchetti presenti nella distribuzione sia per il software esterno [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. 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 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, dandone comunicazione al Servizio Calcolo.

Verifica degli account e delle credenziali

Si consiglia di eseguire periodicamente controlli con programmi specifici (per es. **John The Ripper**) sui file di password degli account utente.

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. A tal fine **È OBBLIGATORIO** utilizzare sempre *sudo* per eseguire comandi di amministrazione [ABSC ID 5.1.2].

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 facente parte del 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, ricorrere all'uso di **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* 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].

Oltre a proteggere il sistema operativo un *antivirus*, anche su sistemi GNU/Linux, è utile ad arginare la diffusione di malware che colpiscono sistemi operativi diversi.

È OBBLIGATORIO l'uso di un *firewall* personale come, ad esempio, `iptables` [ABSC ID 8.1.2].

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 (p.e. 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][7].

Nel caso di backup su *cloud,* o nel caso in cui non sia possibile assicurare la riservatezza delle informazioni mediante adeguata protezione fisica dei supporti **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione [ABSC ID 10.3.1], assicurandosi non sia 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][8].

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.

7 Vedi **Prima copia di sicurezza**
8 La richiesta è volta a migliorare la protezione contro *ransomware* (Reveton, CryptoLocker, WannaCry, ...).

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][9].

Compromissione del sistema

In caso di compromissione del sistema il Servizio Calcolo **DEVE** essere immediatamente informato.

Il ripristino del sistema **DEVE** essere eseguito tramite le immagini salvate a conclusione della fase di installazione e configurazione[10] o come una nuova installazione[11] [ABSC ID 3.2.2].

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.

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

Altre raccomandazioni

Installare software per il controllo dell'integrità dei file di sistema come, ad esempio, **ossec**.

Disabilitare i seguenti servizi o filtrare le porte interessate:

- echo (7/tcp e udp);
- systat (11/tcp);

9 Vedi **Gestione di file con dati critici o "rilevanti" per l'ente**.
10 Vedi **Prima copia di sicurezza**.
11 Vedi **Installazione**.

- chargen (19/tcp e udp);
- rstat (udp);
- tftp (69/udp);
- rwall (udp);
- ruser (udp);
- discard (9/tcp e udp);
- daytime (13/tcp e udp);
- bootps (67/udp);
- finger (79/tcp);
- sprayd (udp);
- pcnfsd (udp);
- netstat (15/tcp);
- who (513/udp).

Controlli periodici:

- 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 device siano dell'utente `root` ad eccezione dei terminali;
- Verificare che nella directory **`/dev`** non siano presenti file "normali";
- 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`

- Verificare la presenza di file `.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`).

Parte II
Sistemi macOS

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[12] per accedere al *Firmware* così da impedire l'avvio da dispositivi esterni e l'accesso alla Recovery Console.

12 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][13].

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 più 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, non essere banali o presenti nei dizionari di qualsiasi lingua [ABSC ID 5.7.1].
- **DEVONO** essere modificate con sufficiente frequenza [ABSC ID 5.7.3].
- **NON DEVONO** essere riutilizzate a breve distanza di tempo [ABSC ID 5.7.4].

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

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

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[14], 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 non appena disponibili [ABSC ID 4.8.2]. Per far questo possono essere impostati aggiornamenti automatici (p.e. tramite `cron`) sia per i pacchetti presenti nella distribuzione sia per il software esterno [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

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

di allarmistica che verifichi la disponibilità di aggiornamenti. 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 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, dandone 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"[15] [ABSC ID 10.1.1].

Nel caso di backup su *cloud,* o nel caso in cui non sia possibile assicurare la riservatezza delle informazioni mediante adeguata protezione fisica dei supporti, **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione [ABSC ID 10.3.1], assicurandosi che non sia accessibile via rete in modo permanente, onde evitare che eventuali attacchi al sistema possano coinvolgere anche tutte le sue copie di sicurezza [ABSC ID 10.4.1][16].

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][17].

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[18] o come una nuova installazione[19] [ABSC ID 3.2.2].

15 Vedi **Prima copia di sicurezza**.
16 La richiesta è volta a migliorare la protezione contro ransomware (Reveton, CryptoLocker, WannaCry, ...).
17 Vedi anche la sezione **Gestione di file con dati critici o "rilevanti" per l'ente**.
18 Vedi **Prima copia di sicurezza**.
19 Vedi **Installazione**.

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 log 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)

Parte III
Sistemi Windows

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 del sistema operativo **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 automatica predisposto dal Servizio Calcolo, **SI DEVONO** utilizzare solamente immagini prelevate dai *repository* ufficiali o fornite dal Servizio Calcolo, verificandone il *checksum.*

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].

n 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

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

Al fine di aumentare la sicurezza del sistema operativo si consiglia di eseguire le seguenti operazioni al primo avvio, possibilmente scollegati dalla rete.

- assicurarsi che il sistema di gestione dei pacchetti verifichi le *signature* dei pacchetti in modo da ridurre la possibilità di installare pacchetti sospetti;
- per 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.

SI DEVONO impostare Group Policy in modo da richiedere che le credenziali (delle utenze amministrative):

- abbiano un'elevata robustezza non essere banali o presenti nei dizionari di qualsiasi lingua[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].

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 Directory 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*

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].

Prima copia di sicurezza

Completata la procedura di installazione e configurazione **SI DEVE** eseguire un backup completo del sistema[20] da utilizzare per ripristinare il sistema in caso di

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

compromissioni[21] [ABSC ID 3.2.2]. Tale backup **DEVE** essere memorizzato *offline* [ABSC ID 3.3.1].

Per gli utenti di 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. 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, dandone comunicazione al Servizio Calcolo.

Verifica degli account e delle credenziali

Al fine di verificare la robustezza delle credenziali eseguire periodicamente controlli con programmi specifici sui file di password degli account utente.

21 Misura non necessaria se l'eventuale ripristino viene sempre fatto a partire dall'immagine originale.

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"[22] [ABSC ID 10.1.1].

Nel caso di backup su *cloud*, o nel caso in cui non sia possibile assicurare la riservatezza delle informazioni mediante adeguata protezione fisica dei supporti, **È OBBLIGATORIO** effettuarne una cifratura prima della trasmissione [ABSC ID 10.3.1], assicurandosi non sia accessibile in modo permanente via rete, onde evitare che eventuali attacchi al sistema possano coinvolgere anche tutte le sue copie di sicurezza [ABSC ID 10.4.1][23].

22 Vedi **Prima copia di sicurezza**.

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[24] o come una nuova installazione[25] [ABSC ID 3.2.2].

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`**

23 La richiesta è volta a migliorare la protezione contro *ransomware* (Reveton, CryptoLocker, WannaCry, ...).
24 Vedi **Prima copia di sicurezza**.
25 Vedi **Installazione**.

- **%SystemRoot%\System32\Winevt\Logs\Setup.evtx**
- **%SystemRoot%\System32\Winevt\Logs\System.evtx**

APPENDICE

Circolare AgID 18/04/2017 , n. 2/2017
GU Serie Generale n.103 del 05-05-2017)

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.