# Misure minime di sicurezza ICT per la Pubblica Amministrazione

VINCENZO CALABRÒ

# Indice

## Misure minime di sicurezza ICT per le PA

- Scopo
- Obiettivo
- Contenuto
- Controlli
- Responsabilità
- Conclusioni

## Finalità

- Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

# Misure Minime di sicurezza ICT per le PA

- Le misure minime di sicurezza ICT, emanate dall'AgID, intendono contrastare le minacce informatiche più comuni e frequenti cui sono soggetti i sistemi informativi della pubblica amministrazione italiana.
- Entro il 31 dicembre 2017 le amministrazioni devono attuare gli adempimenti previsti dalla circolare.

## Approfondimenti

1. Excursus storico
2. Riferimenti normativi

# Scopo

- **La Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015**, da cui scaturiscono le Misure Minime di sicurezza ICT per le Pubbliche Amministrazioni, in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della Pubblica Amministrazione, **sollecita tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi**, secondo una tempistica definita e comunque nel più breve tempo possibile, **di standard minimi di prevenzione e reazione ad eventi cibernetici.**

# Obiettivi

Le misure minime sono un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione in tema di sicurezza delle informazioni e avviare un percorso di monitoraggio e miglioramento.

Le disposizioni:

- forniscono un riferimento operativo direttamente utilizzabile (checklist),
- stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;
- forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;
- responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

# Contenuto 1/2

- Le misure minime di sicurezza sono fortemente ispirate all'insieme di controlli noto come SANS 20, pubblicato dal Center for Internet Security come CCSC "CIS Critical Security Controls for Effective Cyber Defense" nella versione 6.0 di ottobre 2015.
- L'elenco dei 20 controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua.
- L'Agid ritiene (2016) che i primi 5 controlli siano indispensabili per assicurare il livello minimo di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la P.A. italiana.

# Contenuto 2/2

- Poichè il CCSC è stato concepito nell'ottica di prevenire e contrastare gli attacchi cibernetici, non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali.
- Per questa ragione, ai controlli delle prime 5 classi si è deciso di aggiungere quelli della CSC8, relativa alle difese contro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di esfiltrazione.
- Per cui nel documento si fa riferimento a 8 AgID Basic Security Controls (ABSC).

# AgID Basic Security Controls (ABSC)

I controlli sono stati suddivisi in tre gruppi verticali, riferiti a livelli di sicurezza crescente.

1) I controlli del primo gruppo (livello “Minimo”) sono quelli strettamente obbligatori ai quali ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve essere conforme in termini tecnologici, organizzativi e procedurali: essi dunque rappresentano complessivamente il livello sotto al quale nessuna Amministrazione può scendere.
2) I controlli del secondo gruppo (livello “Standard”) rappresentano la base di riferimento per la maggior parte delle Amministrazioni, e costituiscono un ragionevole compromesso fra efficacia delle misure preventive ed onerosità della loro implementazione.
3) I controlli del terzo gruppo (livello “Alto”) rappresentano infine il livello adeguato per le organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati, ma anche l’obiettivo ideale cui tutte le altre organizzazioni dovrebbero tendere.

# Classi di controlli 1/2

- I controlli delle prime due classi (**ABSC 1 e 2**) riguardano rispettivamente **l'inventario dei dispositivi autorizzati e non autorizzati e quello dei software autorizzati e non autorizzati.** In pratica essi impongono all'organizzazione di gestire attivamente i dispositivi hardware e i pacchetti software in uso, predisponendo e mantenendo aggiornati, a diversi livelli di dettaglio e con differenti modalità attuative a seconda del livello di sicurezza, i rispettivi inventari, e prevedendo inoltre meccanismi per individuare e/o impedire tutte le anomalie operative, ossia l'impiego di elementi non noti e/o esplicitamente autorizzati.
- I controlli della terza classe (**ABSC 3**) riguardano **la protezione delle configurazioni hardware e software sui sistemi in uso presso l'organizzazione**.
- I controlli della quarta classe (**ABSC 4**) sono finalizzati ad **individuare tempestivamente, e correggere, le vulnerabilità dei sistemi in uso**, minimizzando la finestra temporale nella quale le vulnerabilità presenti possono essere sfruttate per condurre attacchi contro l'organizzazione.

# Classi di controlli 2/2

- I controlli della quinta classe (**ABSC 5**) sono rivolti alla **gestione degli utenti**, in particolare gli amministratori, ed hanno lo scopo di assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi sui sistemi in uso.
- I controlli della sesta classe (**ABSC 8**) hanno lo scopo di **contrastare l'ingresso e la diffusione nell'organizzazione di codice malevolo** di qualsiasi provenienza.
- I controlli della settima classe (**ABSC 10**) sono relativi alla **gestione delle copie di sicurezza delle informazioni** critiche dell'organizzazione, che in ultima analisi sono l'unico strumento che garantisce il ripristino dopo un incidente.
- L'ottava ed ultima classe (**ABSC 13**) riguarda infine **la protezione contro l'esfiltrazione dei dati** dell'organizzazione, in considerazione del fatto che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

# AgID Basic Security Controls (ABSC)

## Approfondimento

- ABSC 1 (CSC 1): Inventario dei dispositivi autorizzati e non autorizzati
- ABSC 2 (CSC 2): Inventario dei software autorizzati e non autorizzati
- ABSC 3 (CSC 3): Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- ABSC 4 (CSC 4): Valutazione e correzione continua della vulnerabilità
- ABSC 5 (CSC 5): Uso appropriato dei privilegi di amministratore
- ABSC 8 (CSC 8): Difese contro i malware
- ABSC 10 (CSC 10): Copie di sicurezza
- ABSC 13 (CSC 13): Protezione dei dati

# Responsabilità

- L’adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17 ) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017.
- Secondo la circolare, le misure minime di sicurezza devono essere adottate da parte di tutte le pubbliche Amministrazioni entro il 31 dicembre 2017.

# Esempio di modulo di implementazione

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

*Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso*

| ABSC_ID | | # | Descrizione | Modalità di Implementazione | Liv |
|---|---|---|---|---|---|
| 1 | 1 | 1 | Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 | | M |
| | | 2 | Implementare ABSC 1.1.1 attraverso uno strumento automatico | | S |
| | | 3 | Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie. | | A |
| | | 4 | Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico. | | A |
| | 2 | 1 | Implementare il "logging" delle operazione del server DHCP. | | S |
| | | 2 | Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite. | | S |

# Conclusioni

- La norma attuativa prevede che ciascuna Amministrazione debba non solo implementare i controlli rilevanti, ma anche dare brevemente conto della modalità di implementazione compilando un apposito modulo il quale andrà poi firmato digitalmente e conservato dall'Amministrazione e, in caso di incidenti, inviato al CERT-PA.
- Da notare infine che le Misure Minime richiedono che le Pubbliche Amministrazioni accedano sistematicamente a servizi di early warning che consente loro di rimanere aggiornate sulle nuove vulnerabilità di sicurezza.
- Occorre andare oltre le linee guida ed avviare un percorso di risk assessment e, successivamente, adeguare le azioni verso un cyber security by design.

# Approfondimento 1: Excursus storico

- Nel 2002 il Governo ha affidato ad un Comitato di esperti, denominato Comitato Tecnico Nazionale per la sicurezza informatica e delle comunicazioni nella P.A., il compito di redigere le proposte relative alla predisposizione del Piano nazionale della sicurezza ICT e del relativo modello organizzativo per l'incremento dei livelli di sicurezza ICT nelle pubbliche amministrazioni. Il Comitato ha pubblicato nel 2004 un documento denominato "Proposte concernenti le strategie in materia di Sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione".
- Nel 2004 il CNIPA ha costituito un Gruppo di lavoro con l'incarico di redigere il Piano Nazionale della sicurezza delle tecnologie dell'informazione e della comunicazione per la PA e il Modello Organizzativo Nazionale di Sicurezza ICT per la PA. I due documenti rappresentano una prima e concreta azione di promozione della "cultura della sicurezza" nel settore dell'informatica pubblica.
- Il 26 aprile 2016 l'Agid fornisce precise Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni attraverso un documento strutturato intitolato: Misure minime di sicurezza ICT per le Pubbliche Amministrazioni. (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)
- Il 4 aprile 2017 sono giunte in Gazzetta Ufficiale, come allegato alla Circolare AgID n. 1/2017 del 17 marzo 2017, le attese "Misure minime di sicurezza ICT per le pubbliche amministrazioni".
- Il 5 maggio 2017 è stata pubblicata sulla G.U. la circolare AgID n. 2/2017 del 18 aprile 2017 che sostituisce integralmente la precedente circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

# Approfondimento 2: Riferimenti normativi

- Le misure minime per la sicurezza ICT sono emesse in attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri, che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, alla luce dei crescenti rischi cibernetici che minacciano anche il nostro Paese.
- Le misure minime di sicurezza informatica, che costituiscono una parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione di futura emanazione, vengono emanate in forma autonoma, anticipando la loro prossima pubblicazione in Gazzetta Ufficiale mediante i siti web dell'Agenzia e del CERT-PA, al fine di fornire tempestivamente alle PA un riferimento normativo e consentire loro di intraprendere un percorso di verifica ed adeguamento.
- In particolare, la direttiva assegna all'Agid il compito di sviluppare e rendere disponibili degli indicatori precisi rispetto agli standard di riferimento tali da permettere alle amministrazioni di dotarsi degli standard minimi di prevenzione e reazione ad eventi cibernetici.
- L'adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17 ) o, in sua assenza, del dirigente designato.

# Approfondimento 3:

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

*Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso*

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 | ID.AM-1 | X | X | X |
| | | 2 | Implementare ABSC 1.1.1 attraverso uno strumento automatico | ID.AM-1 | | X | X |
| | | 3 | Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie. | ID.AM-1 | | | X |
| | | 4 | Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico. | ID.AM-1 | | | X |
| | 2 | 1 | Implementare il "logging" delle operazione del server DHCP. | ID.AM-1 | | X | X |
| | | 2 | Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite. | ID.AM-1 | | X | X |
| | 3 | 1 | Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete. | ID.AM-1 | X | X | X |
| | | 2 | Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete. | ID.AM-1 | | X | X |
| | 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. | ID.AM-1 | X | X | X |
| | | 2 | Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale. | ID.AM-1 | | X | X |
| | | 3 | Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione. | ID.AM-1 | | | X |
| 1 | 5 | 1 | Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati. | ID.AM-1 | | | X |
| | 6 | 1 | Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale. | ID.AM-1 | | | X |

# Approfondimento 4:

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

*Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione*

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 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'istallazione di software non compreso nell'elenco. | ID.AM-2 | X | X | X |
| | 2 | 1 | Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi. | ID.AM-2 | | X | X |
| | | 2 | Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale). | ID.AM-2 | | X | X |
| | | 3 | Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate. | ID.AM-2 | | | X |
| | 3 | 1 | Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. | ID.AM-2 | X | X | X |
| | | 2 | Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop. | ID.AM-2 | | X | X |
| | | 3 | Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch. | ID.AM-2 | | | X |
| | 4 | 1 | Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete. | ID.AM-2 | | | X |

# Approfondimento 5 (1/2):

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

*Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.*

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 3 | 1 | 1 | Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi. | PR.IP-1 | X | X | X |
| | | 2 | Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate. | PR.IP-1 | | X | X |
| | | 3 | Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco. | PR.IP-2 RC.IM-1 | | | X |
| | 2 | 1 | Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione. | PR.IP-1 | X | X | X |
| | | 2 | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. | PR.IP-2 RC.RP-1 | X | X | X |
| | | 3 | Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti. | PR.IP-3 | | X | X |
| | 3 | 1 | Le immagini d'installazione devono essere memorizzate offline. | PR.IP-2 | X | X | X |
| | | 2 | Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati. | PR.DS-2 PR.IP-2 | | X | X |
| | 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). | PR.AC-3 PR.MA-2 | X | X | X |

# Approfondimento 5 (2/2):

| ABSC | | ID # | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 3 | 5 | 1 | Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati. | PR.DS-6 | | X | X |
| | | 2 | Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert. | PR.DS-6 | | | X |
| | | 3 | Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica. | PR.IP-3 | | | X |
| | | 4 | I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle. | PR.IP-3 | | | X |
| | 6 | 1 | Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate. | PR.IP-3 | | | X |
| | 7 | 1 | Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard. | PR.IP-3 | | | X |

# Approfondimento 6 (1/2):

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

*Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.*

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 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. | ID.RA-1 DE.CM-8 | X | X | X |
| | | 2 | Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura. | ID.RA-1 DE.CM-8 | | X | X |
| | | 3 | Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project). | DE.CM-8 | | | X |
| | 2 | 1 | Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità. | DE.CM-8 | | X | X |
| | | 2 | Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità | DE.CM-8 | | X | X |
| | | 3 | Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile. | DE.CM-8 | | X | X |
| | 3 | 1 | Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione. | DE.CM-8 | | X | X |
| | | 2 | Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente. | DE.CM-8 | | X | X |
| | 4 | 1 | Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. | DE.CM-8 | X | X | X |
| | | 2 | Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione | ID.RA-2 | | X | X |

# Approfondimento 6 (2/2):

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 4 | 5 | 1 | Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni. | PR.MA-1 | X | X | X |
| | | 2 | Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità. | PR.MA-1 | X | X | X |
| | 6 | 1 | Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite. | ID.RA-1 DE.CM-8 | | X | X |
| | 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. | PR.IP-12 RS.MI-3 | X | X | X |
| | | 2 | Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio. | PR.IP-12 RS.MI-3 | | X | X |
| | 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.). | ID.RA-4 ID.RA-5 PR-IP.12 | X | X | X |
| | | 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. | PR.IP-12 | X | X | X |
| | 9 | 1 | Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione. | PR.IP-12 RS.MI-3 | | X | X |
| | 10 | 1 | Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio. | PR.DS-7 | | X | X |

# Approfondimento 7 (1/3):

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

*Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.*

| ABSC | | ID # | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 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. | PR.AC-4 PR.PT-3 | X | X | X |
| | | 2 | Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | PR.AC-4 PR.PT-3 | X | X | X |
| | | 3 | Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa. | PR.AC-4 PR.PT-3 | | X | X |
| | | 4 | Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento. | ID.AM-3 DE.AE-1 | | | X |
| | 2 | 1 | Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. | ID.AM-6 PR.AT-2 DE.CM-3 | X | X | X |
| | | 2 | Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga. | DE.CM-3 | | | X |
| | 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. | PR.IP-1 | X | X | X |
| | 4 | 1 | Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa. | ID.AM-6 PR.IP-3 | | X | X |
| | | 2 | Generare un'allerta quando viene aggiunta un'utenza amministrativa. | ID.AM-6 PR.IP-3 | | X | X |
| | | 3 | Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa. | ID.AM-6 PR.IP-3 | | X | X |
| | 5 | 1 | Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa. | PR.PT-1 DE.AE-1 DE.AE-5 DE.CM-1 | | X | X |

# Approfondimento 7 (2/3):

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 5 | 6 | 1 | Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi. | PR.AC-1 PR.AT-2 | | | X |
| | 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). | PR.AC-1 PR.AT-2 | X | X | X |
| | | 2 | Impedire che per le utenze amministrative vengano utilizzate credenziali deboli. | PR.AC-1 PR.AT-2 | | X | X |
| | | 3 | Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). | PR.AC-1 PR.AT-2 | X | X | X |
| | | 4 | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | PR.AC-1 | X | X | X |
| | | 5 | Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova. | PR.AC-1 | | X | X |
| | | 6 | Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi. | PR.AC-1 PR.AT-2 | | X | X |
| | 8 | 1 | Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi. | PR.AC-1 PR.AT-2 DE.CM-7 | | X | X |
| | 9 | 1 | Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività. | PR.AT-2 PR.PT-2 PR.PT-3 PR.PT-4 | | X | X |

# Approfondimento 7 (3/3):

| ABSC_ID | | # | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 5 | 10 | 1 | Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. | ID.AM-6 | X | X | X |
| | | 2 | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | ID.AM-6 | X | X | X |
| | | 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. | ID.AM-6 PR.AT-2 | X | X | X |
| | | 4 | Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio). | ID.AM-6 PR.AT-2 | | X | X |
| | 11 | 1 | Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. | PR.AC-1 PR.AT-2 | X | X | X |
| | | 2 | Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | PR.AC-1 PR.AC-2 | X | X | X |

# Approfondimento 8 (1/2):

**ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE**

*Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.*

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 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. | DE.CM-4 DE.CM-5 | X | X | X |
| | | 2 | Installare su tutti i dispositivi firewall ed IPS personali. | DE.CM-1 | X | X | X |
| | | 3 | Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati. | DE.AE-3 DE.CM-1 RS.CO-1 RS.MI-1 | | X | X |
| | 2 | 1 | Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione. | PR.IP-3 DE.DP-1 | | X | X |
| | | 2 | È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale. | PR.IP-3 PR.MA-1 PR.MA-2 DE.CM-4 | | X | X |
| | | 3 | L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud. | PR.DS-7 DE.CM-4 | | | X |
| | 3 | 1 | Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. | PR.PT-3 DE.CM-7 | X | X | X |
| | | 2 | Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni. | PR.AC-3 DE.AE-1 DE.CM-7 | | | X |
| | 4 | 1 | Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base. | PR.IP-1 RS.MI-1 RS.MI-2 | | X | X |
| | | 2 | Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi. | PR.IP-1 RS.MI-1 RS.MI-2 | | | X |

# Approfondimento 8 (2/2):

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 8 | 5 | 1 | Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host. | DE.CM-1 DE.CM-4 | | X | X |
| | | 2 | Installare sistemi di analisi avanzata del software sospetto. | DE.CM-4 | | | X |
| | 6 | 1 | Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione. | DE.CM-1 DE.CM-4 | | X | X |
| | 7 | 1 | Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | PR.PT-2 | X | X | X |
| | | 2 | Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | PR.AT-1 DE.CM-4 | X | X | X |
| | | 3 | Disattivare l'apertura automatica dei messaggi di posta elettronica. | PR.AT-1 DE.CM-4 | X | X | X |
| | | 4 | Disattivare l'anteprima automatica dei contenuti dei file. | PR.AT-1 DE.CM-4 | X | X | X |
| | 8 | 1 | Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. | PR.PT-2 DE.CM-4 | X | X | X |
| | 9 | 1 | Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam. | DE.CM-1 DE.CM-4 | X | X | X |
| | | 2 | Filtrare il contenuto del traffico web. | DE.CM-1 DE.CM-4 | X | X | X |
| | | 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). | DE.CM-1 DE.CM-4 | X | X | X |
| | 10 | 1 | Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento. | DE.CM-1 DE.CM-4 | | X | X |
| | 11 | 1 | Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate. | ID.AM-6 DE.CM-4 RS.CO-5 | | X | X |

# Approfondimento 9:

**ABSC 10 (CSC 10): COPIE DI SICUREZZA**

*Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.*

| ABSC_ID # | | | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 10 | 1 | 1 | Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema. | PR.IP-4 | X | X | X |
| | | 2 | Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati. | PR.IP-4 | | | X |
| | | 3 | Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore. | PR.IP-4 | | | X |
| | 2 | 1 | Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova. | PR.IP-4 | | X | X |
| | 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. . | PR.DS-6 | X | X | X |
| | 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. | PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9 | X | X | X |

# Approfondimento 10:

**ABSC 13 (CSC 13): PROTEZIONE DEI DATI**

*Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti*

| ABSC_ID | | # | Descrizione | FNSC | Min. | Std. | Alto |
|---|---|---|---|---|---|---|---|
| 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 | ID.AM-5 | X | X | X |
| | 2 | 1 | Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti | ID.AM-5<br>PR.DS-5 | | X | X |
| | 3 | 1 | Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni. | ID.AM-3<br>PR.AC-5<br>PR.DS-1<br>DE.AE-1 | | | X |
| | 4 | 1 | Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro. | ID.AM-3<br>DE.CM-1 | | | X |
| | 5 | 1 | Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti. | PR.PT-2 | | | X |
| | | 2 | Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi. | ID.AM-1<br>PR.PT-2 | | | X |
| | 6 | 1 | Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie. | ID.AM-3<br>DE.CM-1 | | | X |
| | | 2 | Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line. | ID.AM-3<br>DE.CM-1 | | | X |
| | 7 | 1 | Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto. | ID.AM-3 PR.DS-5<br>DE.CM-1 | | | X |
| | 8 | 1 | Bloccare il traffico da e verso url presenti in una blacklist. | ID.-AM3 PR.DS-5<br>DE.CM-1 | X | X | X |
| | 9 | 1 | Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository. | PR.AC-4<br>PR.DS-5 | | | X |

# Grazie!
# Domande?

VINCENZOCALABRO.IT