CIRCOLARI

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 18 aprile 2017, n. **2/2017**.

Sostituzione della 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)».

Premessa.

L'art. 14-*bis* del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera *a)*, tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

La presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella *Gazzetta Ufficiale* n. 79 del 4 aprile 2017).

Art. 1.

Scopo

Obiettivo della presente circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi.

Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

Art. 2.

Amministrazioni destinatarie

Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3.

Attuazione delle misure minime

Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità della attuazione delle misure minime di cui all'art. 1.

Art. 4.

Modulo di implementazione delle MMS-PA

Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare.

Il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Art. 5.

Tempi di attuazione

Entro il 31 dicembre 2017 le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

Roma, 18 aprile 2017

Il Presidente: SAMARITANI

ALLEGATO *1*

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT

PER LE PUBBLICHE AMMINISTRAZIONI

(*Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015*)

26 APRILE 2016

1. GENERALITÀ.

1.1. SCOPO.

Il presente documento contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni le quali costituiscono parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

Questo documento è emesso in attuazione della direttiva del Presidente del Consiglio dei ministri 1° agosto 2015 e costituisce un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fine di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

1.2 STORIA DELLE MODIFICHE

Ver.	Descrizione delle modifiche	Data emissione
1.0	Prima versione	26/04/2016

1.3 RIFERIMENTI

	ID	Descrizione
[D.1]	Direttiva 1 agosto 2015	Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015
[D.2]	SANS 20	CIS Critical Security Controls for Effective Cyber Defense - versione 6.0 di ottobre 2015
[D.3]	Cyber Security Report	La Sapienza - 2015 Italian Cyber Security Report del CIS -

1.4 ACRONIMI

Acronimo	Descrizione
ABSC	Agid Basic Security Control(s)
CCSC	Center for Critical Security Control
CSC	Critical Security Control
FNSC	Framework Nazionale di Sicurezza Cibernetica
NSC	Nucleo di Sicurezza Cibernetica

2. PREMESSA.

La direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, 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. A fine di agevolare tale processo l'Agenzia per l'Italia digitale è stata impegnata a rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

L'Agenzia è costantemente impegnata nell'aggiornamento continuo della normativa tecnica relativa alla sicurezza informatica della pubblica amministrazione ed in particolare delle regole tecniche per la sicurezza informatica delle pubbliche amministrazioni la cui emanazione è però di competenza del Dipartimento per la funzione pubblica e richiede l'espletamento delle procedure previste dalla normativa comunitaria per la regolamentazione tecnica. Pertanto il presente documento, che contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni e costituisce parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni, viene pubblicato, in attuazione della direttiva sopra citata, come anticipazione urgente della regolamentazione in corso di emanazione, al fine di fornire un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilità per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro è in grado di offrire. L'elenco dei venti 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. È comune convinzione che i primi cinque controlli siano quelli indispensabili per

assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

In realtà nel definire gli AgID Basic Security Control(s) (ABSC) si è partiti dal confronto tra le versioni 6.0 e 5.1 dei CCSC, che può essere assunto quale indicatore dell'evoluzione della minaccia cibernetica nel corso degli ultimi anni. È infatti evidente l'aumento di importanza delle misure relative agli amministratori di sistema, che balzano dal 12° al 5° posto, entrando nella rosa dei Quick Win, mentre la sicurezza applicativa scivola dal 6° al 18° posto e gli accessi wireless dal 7° al 15° a causa della diffusione delle contromisure atte a contrastare le vulnerabilità tipiche di tali ambiti.

In definitiva, anche per facilitare il confronto con la definizione originale, si è deciso di fare riferimento, nell'identificazione degli ABSC, alla versione 6 dei CCSC. Tuttavia l'insieme dei controlli definiti è più vicino a quello della versione 5.1 poiché si è ritenuto che molti di quelli che nel passaggio alla nuova versione sono stati eliminati, probabilmente perché non più attuali nella realtà statunitense, siano ancora importanti nel contesto della pubblica amministrazione italiana.

Occorre inoltre osservare che il CCSC è stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali. Per questa ragione, ai controlli delle prime cinque 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.

In realtà ciascun CSC è costituito da una famiglia di misure di dettaglio più fine, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realtà locale. Nonostante ciò si è ritenuto che anche al secondo livello ci fosse una granularità ancora eccessiva, soprattutto sotto il profilo implementativo, che avrebbe costretto soprattutto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione. Per tale ragione è stato introdotto un ulteriore terzo livello, nel quale la misura di secondo livello viene decomposta in misure elementari, ancora una volta implementabili in modo indipendente. Pertanto un ABSC è identificato da un identificatore gerarchico a tre livelli x, y, z, dove x e y sono i numeri che identificano il CSC concettualmente corrispondente e z individua ciascuno dei controlli di livello 3 in cui questo è stato raffinato.

Al primo livello, che corrisponde ad una famiglia di controlli destinati al perseguimento del medesimo obiettivo, è associata una tabella che li contiene tutti. Nella prima colonna, sviluppata gerarchicamente su tre livelli, viene definito l'identificatore univoco di ciascuno di essi. La successiva colonna «Descrizione» specifica il controllo attraverso una definizione sintetica.

Nella terza colonna, «FNSC» (Framework nazionale di sicurezza cibernetica), viene indicato l'identificatore della Subcategory del Framework Core del Framework nazionale per la Cyber Security, proposto con il 2015 Italian Cyber Security Report del CIS «La Sapienza» presentato lo scorso 4 febbraio 2016, al quale il controllo è riconducibile. Pur non intendendo costituire una contestualizzazione del Framework, le misure minime concretizzano praticamente le più importanti ed efficaci azioni che questo guida ad intraprendere. Per il diverso contesto di provenienza ed il differente obiettivo che i due strumenti intendono perseguire, le misure minime pongono l'accento sopra gli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino.

Le ultime tre colonne sono booleane e costituiscono una linea guida che indica quali controlli dovrebbero essere implementati per ottenere un determinato livello di sicurezza. La prima, «Minimo», specifica il livello sotto il quale nessuna amministrazione può scendere: i controlli in essa indicati debbono riguardarsi come obbligatori. La seconda, «Standard», può essere assunta come base di riferimento nella maggior parte dei casi, mentre la terza, «Alto», può riguardarsi come un obiettivo a cui tendere.

Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.

Le amministrazioni NSC, per l'infrastruttura che gestisce dati NSC, dovrebbero collocarsi almeno a livello "standard" in assenza di requisiti più elevati.

3. LA MINACCIA CIBERNETICA PER LA PUBBLICA AMMINISTRAZIONE.

Nel recente passato si è assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

Se da un lato la pubblica amministrazione continua ad essere oggetto di attacchi dimostrativi, provenienti da soggetti spinti da motivazioni politiche ed ideologiche, sono divenuti importanti e pericolose le attività condotte da gruppi organizzati, non solo di stampo propriamente criminale.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi. Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati. Il secondo è che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti. La combinazione di questi due fattori fa sì che queste misure minime, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attività degli utenti rimangano sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte. Oltre tutto una lunga latenza della compromissione rende estremamente complessa, per la mancanza di log, modifiche di configurazione e anche avvicendamenti del personale, l'individuazione dell'attacco primario, impedendo l'attivazione di strumenti efficaci di prevenzione che possano sicuramente impedire il ripetersi degli eventi.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonché la protezione della configurazione, che è quella immediatamente successiva.

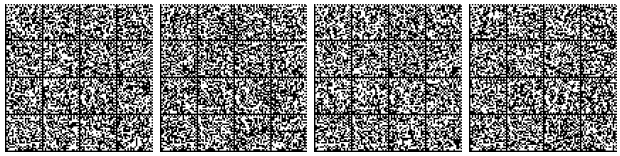
La quarta classe deve la sua priorità alla duplice rilevanza dell'analisi delle vulnerabilità. In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace. Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe è rivolta alla gestione degli utenti, in particolare gli amministratori. La sua rilevanza è dimostrata dall'ascesa, accennata in premessa, dal 12° al 5° posto nelle SANS 20, motivata dalle considerazioni cui si è fatto riferimento poco dianzi.

La sesta classe deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.

Le copie di sicurezza, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.

L'ultima classe, la protezione dei dati, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.



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

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
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

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

[1] Air-gapped: isolato. Tecnica informatica solitamente utilizzata per mettere in sicurezza sistemi o reti che richiedono maggior attenzione rispetto ad altre: basti pensare alle reti classificate come militari, ai sistemi di controllo di grande aziende e industrie sensibili (ad esempio centrali nucleari o industrie chimiche) o *network* che gestiscono e processano pagamenti attraverso carte di credito e bancomat.

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

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

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

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

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

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

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

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

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

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

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 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 PR.AC-5 PR.DS-1 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 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 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 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 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 DE.CM-1			X
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5 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 PR.DS-5			X

ALLEGATO 2

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI

Il presente modello fornisce un ausilio per determinare il livello di copertura prodotto dalle misure poste in essere dall'amministrazione attraverso l'indicazione, nella colonna "Modalità di implementazione", dello strumento effettivamente utilizzato per realizzare lo ABSC riferito alla riga.

Per misura si intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Pertanto, al fine di fornire tutte le principali informazioni identificative e descrittive relative alle singole misure può essere utile fare riferimento anche alle informazioni contenute in procedure, eventualmente, già approvate e adottate dall'Amministrazione che si raccomanda di fornire in allegato in caso di segnalazione di incidente informatico al CERT-PA

Le indicazioni delle modalità di implementazione possono essere ulteriormente utili anche come punto di riferimento dello stato della sicurezza dei servizi/sistemi dell'Amministrazione.

Il modulo deve essere compilato e firmato digitalmente con marcatura temporale dal Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, dal dirigente allo scopo designato e dal Responsabile Legale della struttura.

Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

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	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
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.		M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
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.		M
		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.		S
		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.		A
	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.		A
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.		A

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	Modalità di Implementazione	Liv
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.		M
	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.		S
		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).		S
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.		M
		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.		S
		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.		A
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped[1] 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.		A

[1] Air-gapped: isolato. Tecnica informatica solitamente utilizzata per mettere in sicurezza sistemi o reti che richiedono maggior attenzione rispetto ad altre: basti pensare alle reti classificate come militari, ai sistemi di controllo di grande aziende e industrie sensibili (ad esempio centrali nucleari o industrie chimiche) o *network* che gestiscono e processano pagamenti attraverso carte di credito e bancomat.

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	Modalità di Implementazione	Liv
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.		M
		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.		S
		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.		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
3	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.		M
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.		M
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.		S
	3	1	Le immagini d'installazione devono essere memorizzate offline.		M
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.		S
	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).		M

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
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.		S
		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.		A
		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.		A
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.		A
	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.		A
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.		A

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	Modalità di Implementazione	Liv
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.		M
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.		S
		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).		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
4	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.		S
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità		S
		3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.		S
	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.		S
		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.		S
	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.		M
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione		S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.		M
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.		M
	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.		S
	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.		M
		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.		S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
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.).		M
		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.		M
	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.		S
	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.		S

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	Modalità di Implementazione	Liv
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.		M
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.		M
		3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.		S
		4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.		A
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.		M
		2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
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.		M
	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.		S
		2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.		S
		3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.		S
	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.		S
	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.		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
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).		M
		2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.		S
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).		M
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).		M
		5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.		S
		6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.		S
	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.		S

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

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	Modalità di Implementazione	Liv
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.		M
		2	Installare su tutti i dispositivi firewall ed IPS personali.		M
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.		S
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.		S
		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.		S
		3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
8	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.		M
		2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.		A
	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.		S
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.		A
	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.		S
		2	Installare sistemi di analisi avanzata del software sospetto.		A
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.		S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.		M
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.		M
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.		M
		4	Disattivare l'anteprima automatica dei contenuti dei file.		M
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.		M
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.		M
		2	Filtrare il contenuto del traffico web.		M
		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).		M

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
8	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.		S
	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.		S

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	Modalità di Implementazione	Liv
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il com-		M
		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		A
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfun-		A
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.		S
	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 trasmis-		M
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano		M

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	Modalità di Implementazione	Liv
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		M
	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti		S
	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.		A
	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.		A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
13	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.		A
		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.		A
	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.		A
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.		A
	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.		A
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.		M
	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..		A

17A03060