Misure minime di sicurezza ICT per le pubbliche amministrazioni.
(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)

					Min.	Std.	Alto	Modalità di implementazione
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ								
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	E' codificata una procedura interna, che a fronte di modifiche della infrastruttura o di aggiornamenti dei programmi guida lo svolgimento di test per evidenziare possibili criticità.
4	1	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	
4	1	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	
4	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	DE.CM-8		X	X	
4	2	2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	DE.CM-8		X	X	
4	2	3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	DE.CM-8		X	X	
4	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	
4	3	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	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	Le ricerche di vulnerabilità vengono al momento effettuate utilizzando procedure manuali.
4	4	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	
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	Ove tecnicamente possibile patch e aggiornamenti dei software vengono schedulati in modo automatico:in caso contrario tali aggiornamenti vengono eseguiti manualmente da parte del personale incaricato.
4	5	2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X	X	X	
4	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	
4	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	PR.IP-12 RS.MI-3	X	X	X	Le vulnerabilità evidenziate tramite le procedure di cui al punto 4.1.1 vengono segnalate ad un supervisore che organizza adeguati gruppi di lavoro per risolverle. Una volta applicate le patch viene richiesta una nuova analisi (punto 4.1.1) e confermata la risoluzione al coordinatore.
4	7	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	
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.).	ID.RA-4 ID.RA-5 PR	X	X	X	In sede di definizione delle azioni relative alla nuova normativa in materia di tutela dei dati personali verrà formalizzata una analisi dei rischi e delle relative azioni di mitigazione
4	8	2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	X	Si veda 4.8.1
4	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	
4	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								
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	I privilegi di amministratore sui sistemi server e di sicurezza sono riservati ai responsabili incaricati dell'assistenza , ai tecnici che si occupano della sicurezza. Tali privilegi vengono utilizzati unicamente per lo svolgimento delle attività per le quali essi sono strettamente necessari.
5	1	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	Si veda 5.1.1.
5	1	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	
5	1	4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	ID.AM-3 DE.AE-1			X	
5	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	X	X	X	Le utenze amministrative sono in possesso di soggetti nominati in sede di approvazione delle presenti misure minime.
5	2	2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	DE.CM-3			X	
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.	PR.IP-1	X	X	X	E' normale e ordinaria pratica tecnica ,come tale assicurata dal personale che si occupa delle implementazioni.
5	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X	
5	4	2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X	
5	4	3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X	
5	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	PR.PT-1 DE.AE-1 DE		X	X	
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	
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).	PR.AC-1 PR.AT-2	X	X	X	Le credenziali amministrative utilizzate ,nei limiti di quanto tecnicamente consentito da ogni dispositivo, vengono scelte in modo da garantire elevati livelli di robustezza.
5	7	2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	PR.AC-1 PR.AT-2		X	X	
5	7	3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	PR.AC-1 PR.AT-2	X	X	X	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
5	7	4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	PR.AC-1	X	X	X	Il sistema di autenticazione è configurato per impedire il riutilizzo delle ultime 6 password per tutti gli utenti.
5	7	5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	PR.AC-1		X	X	
5	7	6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	PR.AC-1 PR.AT-2		X	X	
5	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		X	X	
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.	PR.AT-2 PR.PT-2 PR		X	X	

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	Gli utenti interni in possesso di credenziali amministrative dei sistemi server e di sicurezza non operano, per attività ordinarie ,attraverso tali credenziali . Da parte loro i soggetti esterni non hanno necessità di utilizzo di credenziali ordinarie in quanto intervengono solo per esigenze di tipo manutentivo richiedano l'utilizo di credenziali con privilegi elevati .
5	10	2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	ID.AM-6	X	X	X	Ad ogni utenza è attribuito un uid, e in particolare le utenze amministrative sono singole e le credenziali sono personali.
5	10	3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	ID.AM-6 PR.AT-2	X	X	X	Le credenziali amministrative di sistema vengono comunicate e sono utilizzate solo dai tecnici durante gli interventi di gestione dell'infrastruttura.
5	10	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	
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X	Le credenziali amministrative sono in possesso di personale formalmente incaricato e di provata affidabilità.
5	11	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	Non si utilizzano certificati digitali per l'autenticazione .
ABSC 10 (CSC 10): COPIE DI SICUREZZA								
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	Vengono eseguite, con schedulazione quotidiana, copie di sicurezza dei dati presenti sui server dell fornitore di servizio.
10	1	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	
10	1	3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X	
10	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X	
10	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	PR.DS-6	X	X	X	Le copie dei dati sono conservate con un livello di sicurezza allineato a quello del server principale.
10	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.	X	X	X	I supporti contenenti le copie vengono ruotati in modo che quelli non in uso non siano accessibili dal sistema informatico