agosto 2015) vers. 2

					Min.	Std.	Alto	
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI								
ABSC_ID #			**Descrizione**	**FNSC**				**CANOSSA**
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X	Si, inventario eseguito con lansweeper e conservato presso il Servizio Informatico Associato
1	1	2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X	NO
1	1	3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X	NO
1	1	4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X	NO
1	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X	Si, è attivo il log DHCP integrato nel server Microsoft
1	2	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	NO
1	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X	L'elenco della misura 1.1.1 è aggiornato al 31/12/2017
1	3	2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X	NO
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.	ID.AM-1	X	X	X	Vedi punto 1.1.1
1	4	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	NO
1	4	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	NO
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	NO
1	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X	NO
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI								
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	Si, elenco stilato tramite lansweeper e conservato presso il Servizio Informatico Associato.
2	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	Esiste la whitelist ma non c'è un sistema che blocca in automatico l'installazione di altre procedure. Bensì viene eseguito un monitoraggio.
2	2	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	NO
2	2	3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	ID.AM-2			X	NO
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X	Ultima scansione effettuata a dicembre 2017
2	3	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	NO

2	3	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	NO
2	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	NO
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER								
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X	NO
3	1	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	NO
3	1	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	NO
3	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	NO
3	2	2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X	NO
3	2	3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	PR.IP-3		X	X	NO
3	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X	Si di alcuni dispositivi strategici sono create immagini off line
3	3	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	NO
3	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	X	Si, utilizzo di connessioni VPN di tipo SSL
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	NO
3	5	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	NO
3	5	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	NO
3	5	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	NO
3	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	NO
3	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	PR.IP-3			X	NO
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	NO
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	NO
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	NO
4	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	DE.CM-8		X	X	NO
4	2	2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	DE.CM-8		X	X	NO
4	2	3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	DE.CM-8		X	X	NO
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	NO
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	NO
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	Si, la suite F-Secure installata verifica più volte al giorno gli aggiornamenti

			Generale					
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	Si, la suite F-Secure mediante gli aggiornamenti quotidiani può segnalare nuove minacce o necessità di patch per risolvere vulnerabilità
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	Si, ogni pc ha gli aggiornamenti di sistema e delle applicazioni in modalità automatica ma non centralizzata
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	Non sono presenti questo tipo di sistemi
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	Si, mediante le policy di F-Secure
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	Si, attività di analisi per determinate patch legate a gravi vulnerabilità
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	NO
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-IP.12	X	X	X	Si, non appena sono disponibili le patch vengono installate
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
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	Si, intervenendo sul firewall locale o di rete
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	No, non c'è la necessità
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	SI per sistemi server. Le postazioni client vengono gestite con amministratori locali, che possono intervenire solo sulla proprima postazione per limitare danni generalizzati ai sistemi.
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 solo sui sistemi server
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	NO
5	1	4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	ID.AM-3 DE.AE-1			X	NO
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.CM-3	X	X	X	SI
5	2	2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	DE.CM-3			X	NO
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	Si, le credenziali standard vengono sostituite con credenziali personalizzate dall'ente
5	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X	NO
5	4	2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X	NO
5	4	3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X	NO
5	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	Si, i log di windows registrano gli accessi
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	NO
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	SI
5	7	2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	PR.AC-1 PR.AT-2		X	X	SI per gli utenti locali NO per administrator di dominio

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	Si, le credenziali degli utenti sono soggette alle policy su complessità e durata (ogni 3 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	Si, le credenziali degli utenti sono soggette alle policy su complessità e durata (ogni 2 anni)
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	Si, le credenziali degli utenti sono soggette alle policy su complessità e durata
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	Si, le credenziali degli utenti sono soggette alle policy su complessità e durata
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.CM-7		X	X	NO
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.PT-3 PR.PT-4		X	X	NO
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	No, per esigenze di funzionamento di alcuni software gli utenti locali sono impostati come amministratori locali del PC
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	Si, è attivo l'utente administrator generico e sono attivi utenti amministratori di dominio riconducibili alle persone autorizzate
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	SI, ogni utente amministratore che accede ha le proprie credenziali
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	Si, in caso di necessità viene usato l'amministratore di dominio
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X	SI
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	No, non sono in uso certificati
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE								
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	Si, è installata la suite F-Secure
8	1	2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X	Firewall attivo o Microsoft e dell'antivirus
8	1	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	NO
8	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	Si, la console F-Secure gestisce tutto centralmente
8	2	2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi antimalware 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	Si, dalla console è possibile forzare l'esecuzione di operazioni ai client
8	2	3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	PR.DS-7 DE.CM-4			X	Si, la suite F-Secure utilizza anche controlli basati sui servizi in cloud
8	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X	NO
8	3	2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	PR.AC-3 DE.AE-1 DE.CM-7			X	NO
8	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	NO
8	4	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	NO
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	Si, mediante l'uso di proxy trasparente

8	5	2	Installare sistemi di analisi avanzata del software sospetto.	DE.CM-4			X	NO
8	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	DE.CM-1 DE.CM-4		X	X	Si, mediante l'uso di proxy trasparente
8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X	SI l'esecuzione automatica è disabilitata viene chiesta conferma all'utente e l'attivazione dei file è controllata dall'antivirus
8	7	2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X	Si, nei software l'esecuzione di macro è soggetta all'approvazione dell'utente
8	7	3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X	Si, i messaggi di posta vengono visualizzati solo se cliccati
8	7	4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X	dipende dal formato
8	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	No, la scansione viene eseguita al momento dell'apertura di un file non a livello di intero supporto
8	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X	Si, il controllo antispam viene eseguito sia a livello di firewall che a livello di server di posta
8	9	2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X	Si, mediante l'uso di proxy trasparente
8	9	3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	DE.CM-1 DE.CM-4	X	X	X	Si, la posta elettronica è soggetta a filtri così come la navigazione web
8	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	Si, la suite F-Secure utilizza controlli heuristici e controlli basati su servizi in cloud
8	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	Si, nel caso sia necessario è possibile inviare il file sospetto a F-Secure per un'analisi approfondita
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	Si quotidianamente
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	SI sono backup completi
10	1	3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X	Si, quando è possibile il backup viene eseguito con differenti software
10	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X	Si, periodicamente e quando richiesto vengono eseguite operazioni di recupero
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	SI il livello di protezione in linea con i sistemi di cui viene eseguita la copia
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.IP-5 PR.IP-9	X	X	X	Si, i backup non sono direttamente accessibili
ABSC 13 (CSC 13): PROTEZIONE DEI DATI								
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	NO
13	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	NO
13	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	NO
13	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	NO
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.	PR.PT-2			X	NO
13	5	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	NO
13	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	NO
13	6	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	Si, negli apparati di rete sono attive le funzionalità di log

13	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	NO
13	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5 DE.CM-1	X	X	X	Si, mediante l'uso di proxy trasparente
13	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.				X	NO

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

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto	Modalità di implementazione
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI								
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X	Implementazione entro il 25/5/2019 strumento automatico GFI Languard. Nell'inventario saranno inclusi tutti i sistemi e i dispositivi connessi alla rete delle organizzazioni. Le informazioni sui dispositivi saranno aggiornate dopo ogni nuovo polling della rete. L'elenco dei dispositivi dovrà contenere: dispositivi, dispositivi mobili, dispositivi di rete, dispostivi virtuali, perifieriche per computer, dispositivi connetti, telefoni VoIP, archivi di rete. Nell'elenco per ogni dispositivi, saranno riportate le seguenti informazioni: codice identificativo univoco assegnato all'apparato, descrizione breve del tipo di dispositivo, MAC adress, indirizzo IP (se statico, se assegnato dinamicamente indicare tale fatto), collocazione a persona alla quale è assegnato.
1	1	2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X	Vedi punto 1.1.1
1	1	3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X	
1	1	4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X	
1	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X	
1	2	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	
1	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X	Redazione policy di gestione dell'inventario
1	3	2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X	
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.	ID.AM-1	X	X	X	Vedi punto 1.1.1
1	4	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	
1	4	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	
1	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								
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	Implementazione entro il 25/5/2019 strumento automatico GFI Languard Nell'inventario saranno inclusi tutti i software utilizzati all'interno delle organizzazioni. Nell'elenco per ogni software, saranno riportate le seguenti informazioni: tipologi del dispositivo, nome del software, fornitore e/o marca, vesione, soggetto autorizzante, eventuale data di scadenza dell'autorizzazione, informazioni sulla licenza.
2	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	2	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	
2	2	3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	ID.AM-2			X	
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X	Introduzione strumento automatico di scansione e monitoraggio. Redazione policy di gestione e monitoraggio inventario software entro 25/5/2018.
2	3	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	
2	3	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	
2	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	
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER								
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X	Redazione policy entro 30/9/2019 contenente: definizione contenuti immagine sicura per ogni sistema operativo utilizzato, periodicità aggiornamento immagini, ruoli e compiti (amministratore di sistema), luogo di conservazione immagini, modalità di ripristino, connessioni protette e password.

3	1	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	1	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	
3	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	Vedi punto 3.1.1
3	2	2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X	Vedi punto 3.1.1
3	2	3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	PR.IP-3		X	X	
3	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X	Vedi punto 3.1.1
3	3	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	
3	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	X	Vedi punto 3.1.1
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	
3	5	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	5	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	
3	5	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	
3	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	
3	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								
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	Entro il 25/5/2019 implementare sistema di scansione delle vulnerabilità. Entro il 25/5/2019 redazione policy contenente: modalità di scansione delle vulnerabilità, ruoli e compiti (amminsitratore di sistema), modalità e tempistiche di aggiornamento, report delle valutazioni, contromisure, mancati aggiornamenti con motivazioni, tempistiche e modalità (centralizzate oppure manuali per alcuni applicativi) di distribuzione delle patch, modalità di aggiornamento sistemi non raggiungibili tramite rete, verifica risoluzioni delle vulnerabilità
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	Vedi punto 4.1.1
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	Vedi punto 4.1.1
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	Vedi punto 4.1.1
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	Vedi punto 4.1.1
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-IP.12	X	X	X	Definizione del Piano di gestione dei rischi con relativa policy.
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	Vedi punto 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	Redazione entro il 31/03/2019 policy "sistema di autenticazione": gestione delle password, modalità di utlizzo, livelli diversi in base a ruoli e attività, registrazione accessi, registrazione log, autenticazione a più fattori etc. Redazione inventario password, conservazione, formalizzazione e nomina
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	Vedi punto 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.CM-3	X	X	X	Vedi punto 5.1.1
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	Vedi punto 5.1.1
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.AE-5 DE.CM-1		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	Vedi punto 5.1.1
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	Vedi punto 5.1.1
5	7	4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	PR.AC-1	X	X	X	Vedi punto 5.1.1
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.CM-7		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.PT-3 PR.PT-4		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	Vedi punto 5.1.1
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	Vedi punto 5.1.1
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	Vedi punto 5.1.1
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	Vedi punto 5.1.1
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	Vedi punto 5.1.1
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE									
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	Si, è installata la suite F-Secure
8	1	2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X	Si, sui PC è attivo il firewall
8	1	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	
8	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	
8	2	2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi antimalware 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	
8	2	3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	PR.DS-7 DE.CM-4			X	
8	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X	Policy di utilizzo dei dispositivi esterni e attrezzature di lavoro
8	3	2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	PR.AC-3 DE.AE-1 DE.CM-7			X	
8	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	
8	4	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	
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	
8	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	DE.CM-1 DE.CM-4		X	X	
8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X	Si, sui PC l'esecuzione automatica è disabilitata
8	7	2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X	Si, nei software l'esecuzione di macro è soggetta all'approvazione dell'utente
8	7	3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X	Si, i messaggi di posta vengono visualizzati solo se cliccati
8	7	4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X	Si, disattivata
8	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	No, la scansione viene eseguita al momento dell'apertura di un file non a livello di intero supporto
8	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X	Si, il controllo antispam viene eseguito sia a livello di firewall che a livello di server di posta
8	9	2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X	Si, mediante l'uso di proxy trasparente

8	9	3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	DE.CM-1 DE.CM-4	X	X	X	Si, la posta elettronica è soggetta a filtri così come la navigazione web
8	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	
8	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								
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	Le copie di sicurezza vengono effettuate quotidianamente
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	Redazione policy di gestione, cifratura e conservazione copie di sicurezza
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.IP-5 PR.IP-9	X	X	X	Vedi punto 10.3.1
ABSC 13 (CSC 13): PROTEZIONE DEI DATI								
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	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). Gli Enti procederanno all'individuazione degli ambiti di riservatezza che richiederanno la crittografia dei dati.
13	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	
13	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	
13	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	
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.	PR.PT-2			X	
13	5	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	
13	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	
13	6	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	
13	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	
13	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5	X	X	X	Ok
13	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 P			X	