ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Realizzare un archivio delle risorse attive nel quale saranno elencati i dispositivi utilizzati dall'amministrazione. L'archivio è così organizzato: ID Nome PC Collocazione Indirizzo IP Indirizzo MAC Applicativi installati
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	///
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Sarà realizzato, mediante apposito router dotato di sistema operativo RouterOS con DUDE server implementato, per la gestione degli apparati di rete.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	///
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	///
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	///
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Il registro dovrà essere aggiornato tempestivamente per ogni nuova risorsa collegata alla rete.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	///
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Da realizzare, tali dati saranno inseriti nell'archivio delle risorse attive di cui al punto 1.1.1
1	4	2	S	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.	///
1	4	3	A	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.	///
1	5	1	A	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.	///

1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	///

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	MMMM	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	E' stato predisposto un elenco dei software utilizzati su ogni macchina dell'amministrazione. I dispositivi saranno configurati in modo tale che l'utente standard non disponga dei privilegi che permettono liberamente l'installazione del software
2	2	1	SSSS	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.	///
2	2	2	SSSS	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).	///
2	2	3	AAAA	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	///
2	3	1	MMMM	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodicamente (almeno una volta ogni 6 mesi) saranno realizzate dei controlli per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1.
2	3	2	SSSS	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	///
2	3	3	AAAA	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.	///
2	4	1	AAAA	Utilizzare macchine virtuali e/o sistemi air-gapped 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.	///

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	MMMM	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Per sistemi desktop e server si definirà la dotazione software standard e i criteri per gruppi omogenei attraverso policy per gestire le richieste di autenticazione per la sicurezza.
3	1	2	SSSS	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.	///
3	1	3	AAAA	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.	///
3	2	1	MMMM	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Si effettuerà la configurazione tramite procedure standard predisposte dall'ufficio Servizi Informatici
3	2	2	MMM	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso in cui un dispositivo risulti compromesso sarà ripristinato alla configurazione standard.
3	2	3	SSS	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	///
3	3	1	MMM	Le immagini d'installazione devono essere memorizzate offline.	Utilizzo NAS/ HDD esterno per la memorizzazione delle immagini dei server o client particolarmenti importanti.
3	3	2	SSS	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	///
3	4	1	MMM	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)	Tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri
3	5	1	SSS	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.	///
3	5	2	AAA	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.	///

3	5	3	AAA	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.	///
3	5	4	AAA	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	///
3	6	1	AAA	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	///
3	7	1	AAA	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	///

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	MMM	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.	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei dispositivi.
4	1	2	SSS	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	///
4	1	3	AAA	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).	///
4	2	1	SS	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	///
4	2	2	SS	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	///
4	2	3	SS	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	///
4	3	1	SS	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.	///
4	3	2	SS	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.	///
4	4	1	MM	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	I software di ricerca delle vulnerabilità sono regolarmente aggiornati (Almeno una volta al mese saranno controllati gli aggiornamenti dei software utilizzati per la scansione delle vulnerabilità)
4	4	2	SS	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione.	///

4	5	1	MM	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Le macchine sono configurate per gli aggiornamenti automatici del software sia per il sistema operativo sia per le applicazioni.
4	5	2	MM	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	///
4	6	1	SS	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	///
4	7	1	MM	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.	Sarà predisposto un registro dove annotare le eventuali vulnerabilità riscontrate e come siano state risolte (i.e. attraverso l'installazione di patch o ripristinando il dispositivo)
4	7	2	SS	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.	///
4	8	1	MM	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.).	Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione. Esistono procedure automatizzate di backup per la salvaguardia dei dati residenti in sede.
4	8	2	MM	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.	Il pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza.
4	9	1	SS	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.	///
4	10	1	S	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.	///

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Si sta procedendo a verificare che l'accesso ai dispositivi da parte degli utenti non avvenga con accessi amministrativi e ove lo fosse a convertire l'utenza in una non amministrativa.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione (si registreranno gli accessi che richiedano i privilegi specificando le relative operazioni).
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	///
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	///
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Ogni dispositivo avrà una sola utenza amministrativa (Sarà predisposto un registro con tutte le utenze amministrative attive e non attive, data autorizzazione e validità e relativa password assegnata. Tale elenco dovrà essere custodito in cassaforte e messo a disposizione solo al personale addetto alla manutenzione dei dispositivi. Le password dovranno essere non banali e di almeno 14 caratteri di lunghezza).
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	///
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Dopo l'installazione di un nuovo dispositivo sarà cambiata la password di default dell'utente amministratore con un livello di sicurezza almeno pari a quello specificato al punto 5.2.1
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	///
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	///
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	///
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	///
5	6	1	A	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.	///

5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Le password utilizzate per le utenze amministrative sono lunghe almeno 14 caratteri e non banali.
5	7	2	SSSS	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	///
5	7	3	MMMM	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le password per le utenze amministrative saranno periodicamente aggiornate. (viene imposta una scadenza trimestrale o semestrale in funzione del grado di criticità).
5	7	4	MMMM	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non è possibile riutilizzare password precedentemente utilizzate.
5	7	5	SSSS	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	///
5	7	6	SSSS	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	///
5	8	1	SSSS	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.	///
5	9	1	SSSS	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.	///
5	10	1	MMMM	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Si assicura che c'è la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori.
5	10	2	MMMM	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Sono associate a nome e cognome degli utenti ad ogni credenziale di accesso.
5	10	3	MMMM	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.	Le password degli account di amministratore predefinito dei sistemi sono custodite dal custode delle password e in mancanza di designazione dal DSGA. L'utilizzo di tali credenziali è annotato in un apposito registro
5	10	4	SSSS	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	///
5	11	1	MMMM	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate in cassaforte ed accessibili solo al responsabile della struttura ed al direttore sga.

5	11	2	MMMM	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano per l'accesso certificati digitali.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	MMMM	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.	Su tutti i dispositivi sono installati sistemi atti a rilevare la presenza e bloccare l'esecuzione di malware e sono aggiornati automaticamente
8	1	2	MMM	Installare su tutti i dispositivi firewall ed IPS personali.Installare su tutti i dispositivi firewall ed IPS personali.Installare su tutti i dispositivi firewall ed IPS personali.	Tutti i dispositivi sono forniti, se disponibile per il particolare dispositivo, di software firewall o IPS (Intrusion prevention systems) personale al momento della messa in esercizio.
8	1	3	SSS	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	///
8	2	1	SSS	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	///
8	2	2	SSS	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.	///
8	2	3	AAA	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	///
8	3	1	MMM	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è consentito l'uso di dispositivi esterni nella rete amministrativa se non in casi di emergenza
8	3	2	AAA	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	///
8	4	1	SSS	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.	///
8	4	2	AAA	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	///
8	5	1	SSS	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	///
8	5	2	AAA	Installare sistemi di analisi avanzata del software sospetto.	///
8	6	1	SSS	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	///

8	7	1	MMM	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Disattivata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	MMM	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Disattivata l'esecuzione automatica dei contenuti dinamici presenti nei file
8	7	3	MMM	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Disattivata l'apertura automatica dei messaggi di posta elettronica
8	7	4	MMM	Disattivare l'anteprima automatica dei contenuti dei file.	Disattivata l'anteprima automatica dei contenuti dei file.
8	8	1	MM	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Al momento della connessione di supporti rimovibili sarà eseguita automaticamente una scansione anti-malware
8	9	1	MM	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Prima che i messaggi di posta elettronica vengono acquisite dal sistema documentale sarà eseguita una prima analisi sul dominio **@comune.canicatti.ag.it** utilizzandone il servizio antispam ed antivirus in dotazione a ogni singola casella mail
8	9	2	MM	Filtrare il contenuto del traffico web.	Il contenuto del traffico web sarà filtrato attraverso un proxy server /firewall
8	9	3	MM	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).	Bloccati nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa.
8	10	1	SS	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	///
8	11	1	SS	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.	///

ABSC 10 (CSC 10): COPIE DI SICUREZZA					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	MM	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto per le banche dati presenti nell'amministrazione. Per gli altri dati e per le immagini di sistema si attiverà un
10	1	2	AA	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.	///
10	1	3	AA	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	///
10	2	1	SS	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	///
10	3	1	MM	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.	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto per le banche dati presenti nell'amministrazione. Per gli altri dati e per le immagini di sistema si attiverà un sistema NAS con cifratura e posizionamento dello stesso in luogo sicuro.
10	4	1	MM	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.	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto per le banche dati presenti nell'amministrazione. Per gli altri dati e per le immagini di sistema si attiverà un sistema NAS con cifratura e posizionamento dello stesso in luogo sicuro.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	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	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto per le banche dati presenti nell'amministrazione. Per gli altri dati e per le immagini di sistema si attiverà un sistema NAS con cifratura e posizionamento dello stesso in luogo sicuro.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	///
13	3	1	A	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.	///
13	4	1	A	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.	///
13	5	1	A	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.	///
13	5	2	A	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.	///
13	6	1	A	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.	///
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	///
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	///
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall/proxy server

13	9	1	A	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.	///