

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	I sistemi client, server, dispositivi mobili e dispositivi di rete di proprietà dell'Ente sono innanzitutto inventariati come previsto dall'attività di registrazione dei cespiti. Su fogli elettronici sono raccolte tutte le informazioni relative alle postazioni di lavoro sia fisse che portatili.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Non è attualmente previsto l'uso di sistemi automatici.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Non sono attivi sistemi in grado di notificare il collegamento alla rete di nuovi dispositivi non previsti ed eventualmente riconosciuti come anomalie. È comunque garantita la possibilità di rilevare qualunque dispositivo connesso alla rete.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Non viene effettuata un'analisi sistematica e/o periodica del traffico al fine di qualificare i sistemi. Tale tipo di analisi risulta particolarmente onerosa e viene effettuata unicamente a seguito di segnalazione di eventi specifici che necessitano di attenzione e monitoraggio.
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Gli apparati di servizio a cui viene rilasciato indirizzo ip tramite server DHCP vengono registrati nel log di sistema.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Periodicamente viene analizzato il file di log, ma non viene utilizzato per migliorare l'inventario in quanto si tratta di assegnazioni temporanee.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Vengono aggiornati i fogli excel. Il collegamento alla rete Comunale dei dispositivi autorizzati segue una procedura standardizzata che prevede, tra i suoi adempimenti, l'inserimento di ciascuna postazione affidata ai dipendenti nel dominio al fine di garantirne la gestione e configurazione. Non esistono procedure specifiche per l'identificazione di altre tipologie di device (es. dispositivi mobili smartphone e tablet o computer portatili BYOD).
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Non è attualmente previsto l'uso di sistemi automatici.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla	L'inventario delle attrezzature su fogli excel include l'indirizzo IP

				rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	delle macchine. Non è attualmente disponibile un inventario dei dispositivi mobili smartphone e tablet aziendali e BYOD.
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.	Sono in fase di aggiornamento le informazioni dell'attuale inventario su fogli excel.
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.	Attualmente non sono in uso strumenti automatici e/o manuali per la gestione dell'inventario di dispositivi mobili smartphone e tablet sia aziendali che BYOD.
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.	E' prevista un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non è attiva alcuna gestione dei certificati per l'autenticazione dei client.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	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.	Non esiste un elenco del software formalmente autorizzato. Esistono inoltre indicazioni su versione dei sistemi operativi e sul software che deve essere installato sulle postazioni di lavoro in relazione al reparto di appartenenza e alle eventuali licenze disponibili. Poiché gli utenti non hanno di norma diritti amministrativi non è loro consentito installare software in autonomia.

					Non è attualmente disponibile un elenco delle applicazioni installate sui dispositivi mobili smartphone e tablet aziendali e
2	2	1	S	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.	Non è definita alcuna whitelist poiché non è stata stabilita una definizione formale di "software autorizzato".
2	2	2	S	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).	Sui server con funzionalità specifiche vengono installate unicamente le applicazioni strettamente necessarie al funzionamento dei relativi servizi. Sulle postazioni di lavoro non è prevista l'installazione di software personalizzato.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Attualmente non viene implementata la verifica di integrità dei file delle applicazioni installate.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Nessun utente ha le autorizzazioni per installare in autonomia alcun tipo di software.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	E' mantenuto su foglio excel l'elenco dei software utilizzati.
2	3	3	A	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.	Non sono disponibili strumenti automatici di inventario del software.
2	4	1	A	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.	Non sono presenti applicazioni critiche che rendano necessario l'isolamento dalla rete. Qualora fossero richieste sarebbero utilizzabili sistemi virtuali.

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	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Sia le postazioni di lavoro che i server vengono installati con configurazioni standard tali da garantire un livello di sicurezza adeguato. Non è prevista una configurazione standard per quanto riguarda i dispositivi mobili smartphone e tablet.
3	1	2	S	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.	<p>A partire da sistemi operativi più recenti, sia client che server, la protezione della memoria su heap e stack è attiva di default.</p> <p>Le patch dei sistemi Microsoft supportati sono applicate in modo automatico tramite sistema WSE.</p> <p>Non è prevista una procedura di hardening per quanto riguarda i dispositivi mobili smartphone e tablet.</p>
3	1	3	A	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.	Le immagini d'installazione vengono tipicamente aggiornate ad ogni fornitura significativa di hardware delle postazioni di lavoro. Ad eccezione di necessarie specifiche progettuali, i server sono installati attraverso le immagini delle ultime versioni del sistema operativo.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Sia i client che i server vengono installati secondo una configurazione standard come da procedura.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	I sistemi compromessi vengono ripristinati come da procedura a partire da copie di backup integre e da immagini di installazione standard.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	La procedura di gestione dei cambiamenti e aggiornamento della configurazione standard nelle procedure di configurazione sia per sistemi client che per sistemi server viene attuata.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione sono mantenute in aree con accesso riservato alle sole persone autorizzate
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Le immagini di installazione sono mantenute in aree con accesso riservato alle sole persone autorizzate.

3	4	1	M	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).	Tutti i sistemi sono amministrati attraverso connessioni protette e ritenute sicure (SSH, HTTPS).
3	5	1	S	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.	Tutti i sistemi operativi Microsoft più recenti, sia client che server, assicurano la protezione dei file critici di sistema e garantiscono procedure di ripristino in caso di alterazione.
3	5	2	A	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.	L'alterazione di file di sistema genera un record nel file di log. Non sono tuttavia attivi alert a livello centralizzato.
3	5	3	A	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.	Nei log di sistema sono tracciate eventuali alterazioni di configurazione della macchina e l'autore di tali modifiche. Tuttavia il sistema di segnalazione non permette di visualizzare una cronologia dei cambiamenti di configurazione.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Non sono di norma previsti controlli di integrità.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Non è attualmente previsto un sistema centralizzato di controllo automatico.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Il ripristino delle impostazioni di configurazione standard viene effettuato senza strumenti di gestione.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	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.	Il controllo delle vulnerabilità viene garantito dall'aggiornamento periodico effettuato automaticamente dalla presenza di software antivirus.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità	La ricerca di vulnerabilità non è eseguita secondo una schedulazione periodica ma a seguito di segnalazione di nuove

				dell'infrastruttura.	vulnerabilità o di significative modifiche della configurazione dei sistemi.
4	1	3	A	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).	Non presente
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non vengono attualmente effettuate scansioni di vulnerabilità.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Non vengono attualmente effettuate scansioni di vulnerabilità.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Non vengono attualmente effettuate scansioni di vulnerabilità.
4	3	1	S	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.	Non vengono attualmente effettuate scansioni di vulnerabilità.
4	3	2	S	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.	Non vengono attualmente effettuate scansioni di vulnerabilità.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Tramite WSE tutti i sistemi operativi vengono costantemente aggiornati dalle vulnerabilità identificate. Analogamente il sistema centralizzato di gestione dell'antivirus garantisce la sicurezza delle postazioni di lavoro e dei server.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Vengono ricevute informazioni sulle nuove minacce e vulnerabilità in ambiente windows tramite il servizio prodotto da Microsoft.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Nei sistemi Microsoft, WSE gestisce la verifica e l'installazione automatica degli aggiornamenti critici e delle patch di sicurezza del sistema operativo e delle applicazioni Microsoft. La gestione delle patch sui sistemi server è semiautomatica in modo da garantire la continuità dei servizi attivi. Negli apparati di rete le patch sono installate manualmente

					quando necessario. Attualmente non esiste una gestione centralizzata delle patch relative alle applicazioni non Microsoft.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono presenti sistemi isolati dalla rete poiché non ne sussistono le necessità.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Non sono presenti policy che regolamentano le attività di scansione eseguite con privilegi amministrativi
4	7	1	M	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.	Il personale adibito alla gestione della sicurezza informa il personale IT delle principali vulnerabilità e minacce e, in accordo con esso, pianifica e verifica l'esecuzione delle relative contromisure.
4	7	2	S	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.	La valutazione delle condizioni di sicurezza viene effettuata sporadicamente e limitata a specifici ambiti per necessità contingenti.
4	8	1	M	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.).	Ad oggi si adottano strumenti e tecnologie la cui funzione è quella di proteggere i sistemi informatici dagli attacchi dall'esterno tramite firewall.
4	8	2	M	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.	Per i sistemi client e server la procedura automatica prevede l'applicazione di tutte le patch relative ai rischi di sicurezza e di quelle ritenute critiche.
4	9	1	S	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.	In caso di nuove vulnerabilità critiche note, il personale adibito alla gestione della sicurezza si occupa di attivare tutte le misure alternative volte a contrastare un possibile incidente di sicurezza e a minimizzare eventuali conseguenti problematiche.
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.	Le patch dei prodotti non standard sono testate in ambienti di test 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.	Le utenze di amministrazione sono assegnate solo a personale idoneo e competente.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Gli amministratori di sistema utilizzano utenze standard per svolgere operazioni ordinarie e utenze amministrative per operazioni che richiedono privilegi più elevati. Gli accessi sono quotidianamente loggati.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	A ciascuna utenza amministrativa sono assegnati 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.	Le attività svolte dalle utenze amministrative vengono quotidianamente memorizzate.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'inventario delle utenze amministrative è aggiornato ad ogni nuova assegnazione formalmente autorizzata.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Attualmente non sono operativi strumenti automatici di segnalazioni di variazione.
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.	Prima di collegare alla rete un nuovo dispositivo le credenziali di amministratore predefinite vengono modificate secondo le policy delle password previste.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Non viene tracciata l'aggiunta o la soppressione di un'utenza amministrativa.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Non viene generata allerta quando viene aggiunta un'utenza amministrativa.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Non viene generata 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.	Gli eventi legati ai tentativi falliti di accesso sono tracciati nei log
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.	Sono attualmente adottati meccanismi di autenticazione a più fattori.
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).	La lunghezza minima delle password degli amministratori è attualmente impostata a 8 caratteri.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Tutte le utenze, comprese quelle amministrative, devono soddisfare i requisiti di password complexity stabiliti.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le policy impongono la modifica delle password almeno ogni 90 giorni, come prescritto del Garante per la protezione dei dati personali.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le policy impediscono il riutilizzo delle 5 password precedentemente impostate.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	A seguito della modifica delle credenziali occorre attendere almeno 24 ore per effettuarne una nuova.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Attualmente il periodo di riutilizzo delle password non è impostato a sei mesi.
5	8	1	S	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.	Sono utilizzate utenze amministrative esclusivamente per attività che ne richiedono i privilegi.
5	9	1	S	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.	Le macchine utilizzate per operazioni con privilegi amministrativi non sono esposte direttamente a internet. Si tratta di macchine utilizzate direttamente dal personale addetto alla gestione dei sistemi informativi, tuttavia non sono esclusivamente dedicate a tali operazioni.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Le utenze amministrative sono destinate esclusivamente ai gestori dei sistemi informativi e completamente distinte dalle utenze che non svolgono tali attività.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Sia le utenze standard che quelle amministrative sono personali.

5	10	3	M	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.	Di norma le utenze amministrative "root" e "Administrator" sono utilizzate solo in caso di emergenza.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Si predilige l'uso di utenze amministrative di livello più elevato per l'accesso ai sistemi.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Attualmente le proprie credenziali amministrative sono conservate a cura di ciascun amministratore di sistema.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Le chiavi sono adeguatamente protette.

ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	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.	Tutti i sistemi gestiti centralmente e collegati alla rete locale sono dotati di sistemi antivirus e aggiornati in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i dispositivi è installato un firewall
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Attualmente non esistono sistemi di archiviazione degli eventi attraverso un repository centrale
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Tutti gli strumenti di sicurezza sono gestiti centralmente da amministratori di sistema in modo che agli utenti sia inibita l'alterazione della configurazione.
8	2	2	S	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.	L'aggiornamento non è automaticamente verificato e riportato alla console centrale.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Non è definita una procedura di analisi dei malware. Le informazioni relative a potenziali programmi malevoli sono reperite da siti internet dedicati.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le	Non è generalmente consentito l'uso di dispositivi esterni a quelli

				attività aziendali.	necessari per le attività aziendali.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Attualmente non è previsto il monitoraggio dei dispositivi esterni di memorizzazione delle informazioni.
8	4	1	S	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.	Tutti i sistemi operativi più recenti attualmente in uso implementano nativamente funzionalità di ASLR e DEP. Non è al momento prevista l'applicazione di tali impostazioni tramite i sistemi di gestione centralizzata, ma sono attive nella maggior parte dei sistemi di recente installazione.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Non sono attualmente in uso strumenti aggiuntivi di contrasto alle vulnerabilità.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Il traffico che attraversa i firewall, in particolare il flusso internet in transito nel proxy web, viene analizzato a livello di contenuto permettendo il filtraggio di eventuale codice malevolo.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Al momento non sono implementate soluzioni di analisi avanzata del software sospetto, ma nei nuovi sistemi operativi viene chiesta autorizzazione a tale operazione.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Tutto il traffico web è filtrato da sistemi di content filtering basati anche su liste di indirizzi con cattiva reputazione.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'esecuzione automatica dei contenuti dei dispositivi removibili è disabilitata per tutti i sistemi Microsoft Windows client/server più recenti.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	In tutti i sistemi Microsoft Windows client/server e nelle applicazioni più recenti è richiesta all'utente l'autorizzazione all'esecuzione di contenuti dinamici.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il sistema di posta elettronica in uso impedisce l'apertura automatica dei messaggi come impostazione di default.

8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Una policy specifica impedisce l'anteprima automatica del contenuto dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Tutti i sistemi antivirus in uso prevedono la scansione dei supporti rimovibili prima del loro utilizzo.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	L'intero flusso di posta del comune proveniente dall'esterno viene filtrato da sistemi antispam.
8	9	2	M	Filtrare il contenuto del traffico web.	Tutto il traffico web del comune è filtrato da sistemi avanzati di content filtering.
8	9	3	M	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).	L'intero flusso di posta del Comune proveniente dall'esterno viene filtrato da sistemi antispam configurati in modo da bloccare estensioni di file potenzialmente pericolosi.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Tutti gli antivirus utilizzati sia per i sistemi server sia per sistemi client adottano tecniche di rilevazione euristiche ma non una tecnologia avanzata di rilevamento basata sulle anomalie di comportamento rispetto alla normale attività.
8	11	1	S	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.	In casi di eccezionale e potenziale grave criticità si è provveduto all'invio di campioni di software al produttore dell'antivirus in dotazione.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Giornalmente viene effettuato il backup di tutti i server comunali. Il backup viene replicato su un ulteriore NAS.
10	1	2	A	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.	I backup che comprendono sistema operativo, applicazioni e dati sono effettuati regolarmente sui sistemi server nei quali tale operazione è ritenuta necessaria.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	I backup sono effettuati tramite uno strumento di comprovata affidabilità. Non si ritiene al momento necessario l'impiego di

					strumenti supplementari da affiancare al sistema attualmente adottato.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Il sistema di gestione esegue automaticamente la verifica periodica della consistenza dei backup. L'attività di ripristino viene effettuata quando espressamente richiesta.
10	3	1	M	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 supporti fisici di conservazione dei backup sono adeguatamente protetti in locali chiusi accessibili al solo personale. Non viene effettuata attività di cifratura.
10	4	1	M	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 backup full di lungo periodo sono mantenuti offline su dispositivi di memoria fisica.

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	Non è prevista una attività sistematica di analisi e classificazione delle informazioni gestite dall'ente.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Non sono attive procedure che prevedano la cifratura dei dati su dispositivi portatili poiché, da policy di sicurezza, tali device non dovrebbero contenere 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.	Il traffico crittografato in uscita dall'ente non è sottoposto ad attività di monitoraggio e verifica.
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi	Non sono attualmente previste scansioni in grado di rilevare sui

				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.	server la presenza di dati rilevanti non cifrati. Non esiste una specifica analisi dei dati che permetta di riconoscere specifici "data pattern" per dati sensibili e/o rilevanti.
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.	Non sono presenti indicazioni riguardanti dispositivi esterni di memorizzazione di proprietà dell'ente. Non sono in ogni caso implementati sistemi che ne impediscano l'utilizzo.
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.	Ad oggi non sono in uso strumenti che consentano la scrittura solo su dispositivi autorizzati in base a proprietà che li identifichino in maniera univoca.
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.	Sono presenti strumenti con funzionalità DLP in grado di monitorare i flussi di dati e rilevare eventuali anomalie.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Sono presenti strumenti con funzionalità DLP in grado di eseguire un'analisi automatica della tipologia di dati in transito sulla rete.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Non viene effettuato alcun monitoraggio finalizzato a individuare eventuale traffico cifrato in uscita non previsto.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Tutto il traffico internet è filtrato da sistemi avanzati di content filtering in grado di bloccare i flussi da e verso URL non autorizzate.
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.	Sono presenti strumenti DLP in grado di mantenere le limitazioni di accesso anche sui dati trasferiti al di fuori del loro repository originale.