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	Implementato file formato EXCEL denominato “ABSC_ID_111-Inventario.XLSX” reperibile sul server “CASFILE” percorso di rete \\uffici\tributi e informatica\misure minime sicurezza L’inventario riporta i seguenti dati: - Ubicazione del Bene; - Marca e Modello; - Utente utilizzatore/assegnatario; - IP di rete configurato; - N/S seriale / numero di cespite L’inventario sarà riportato anche nella documentazione prevista dal GDPR nella sezione “ASSET”
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Non Prevista Implementazione possibile prevista nel “PIANO TRIENNALE INFORMATIZZAZIONE”
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Attualmente previsto solo per il server denominato “CASFILE”, con strumento “PANDA SYSTEMS MANAGEMENT”, non previsto sui server: - Polizia Locale; - Biblioteca; - Sociale; - Non previsto sulle Postazioni utente. Implementazione dei server e postazioni attualmente non gestite prevista nel “PIANO TRIENNALE INFORMATIZZAZIONE”

1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Unica Analisi Attuale del traffico di rete è effettuata dal firewall sul traffico tra LAN e WAN Le postazioni potranno essere qualificate e analizzate tramite la rete con le implementazioni previste nel “PIANO TRIENNALE INFORMATIZZAZIONE”
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Previsto in quanto il server DHCP è un servizio gestito dal Firewall che memorizza tutti i log delle operazioni. Inoltre i log di management della rete sono registrati sul Log Manager installato nella rete.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Non gestito, tale attività sarà gestita con altro tipo di strumento e non con il logging.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L’elenco di cui alla misura 1.1.1 è aggiornato. L’aggiornamento dell’elenco è a carico degli Amministratori di Sistema.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Previsto sistema di aggiornamento Automatico degli apparati interconnessi alla rete come da “PIANO TRIENNALE INFORMATIZZAZIONE”
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.	Vedi 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.	Previsto come da inventario Allegato "ABSC_ID_111-Inventario.XLSX" reperibile sul server "CASFILE" percorso di rete \\uffici\tributi e informatica\misure minime sicurezza
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 gestito, in fase di valutazione nell'adeguamento previsto dalla norma Europea - GDPR 2016/679
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.	Non trattandosi di una rete pubblica, alla quale hanno accesso utenti non autorizzati, qualunque dispositivo venga connesso alla rete è autorizzato in quanto dispositivo che deve connettersi. In ogni caso anche i dispositivi connessi alla rete locale del comune sono soggetti alle limitazioni determinate da: - Autenticazione Utente; - Accesso ai server di rete tramite abilitazione specifica sulle policy del dominio di rete; - Regole di filtro sul NAT verso il WWW; - Abilitazione al traffico verso il WWW con la gestione delle tabelle di autorizzazione come policy del firewall. Eventuali altre modalità sono in fase di valutazione in riferimento GDPR 2016/679 ed eventualmente implementabile in riferimento al "PIANO TRIENNALE INFORMATIZZAZIONE"
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non applicato in fase di valutazione con l'adeguamento alla norma Europea - GDPR 2016/679 ed eventualmente implementabile in riferimento al "PIANO TRIENNALE INFORMATIZZAZIONE"

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.	Implementato file formato EXCEL denominato "ABSC_ID_211Inventario SW.XLSX" reperibile sul server "CASFILE" percorso di rete \\uffici\tributi_e_informatica\misure minime sicurezza L'inventario riporta i seguenti dati: Software Licenziati - Software Installati sui Server - Sistema Operativo Installato sui Client "in fase di implementazione" - Software Applicativi installati sui Cliente "in fase di implementazione" Software Free/Open Source - Software Installati sui Server - Sistema Operativo Installato sui Client "in fase di implementazione" - Software Applicativi installati sui Cliente "in fase di implementazione" L'inventario sarà riportato anche nella documentazione prevista dal GDPR nella sezione "ASSET"
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 necessaria in quanto tutte le postazioni sono accedibili dall'utente con password di livello non autorizzato all'installazione di alcun tipo di software. Tale attività è prerogativa esclusiva del personale adibito all'amministrazione della rete.

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).	Casistica non prevista nella rete del Comune di Casatenovo. Applicata se necessaria in future modificazioni delle esigenze della rete e sempre tenendo in considerazione quanto al punto 2.2.1
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Casistica non prevista
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Tenendo in considerazione quanto al punto 2.2.1, gli amministratori di rete, durante i controlli periodici verificano eventuali software non censiti che se presenti sono comunque stati autorizzati dall'amministrazione stessa. Inoltre il Software Antivirus presente sulle postazioni esegue un controllo dei tentativi di installazione di alcuni software chiedendo all'utente che tenta l'installazione di inviare una richiesta di sblocco, ad esempio per i driver delle periferiche. L'eventuale upgrade con "PANDA SYSTEMS MANAGEMENT", previsto ora solo sul server "CASFILE" consentirà un monitoraggio dei software in modalità automatica. Tale implementazione fa parte delle valutazioni previste ne "PIANO TRIENNALE DI INFORMTIZZAZIONE"
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.	Implementato file formato EXCEL denominato "ABSC_ID_211Inventario SW.XLSX" reperibile sul server "CASFILE" percorso di rete \\uffici\tributi e informatica\misure minime sicurezza L'inventario riporta i seguenti dati: Software Licenziati - Software Installati sui Server - Sistema Operativo Installato sui Client "in fase di implementazione"

					- Software Applicativi installati sui Cliente “in fase di implementazione”
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.	L’eventuale upgrade con al “PANDA SYSTEMS MANAGEMENT”, previsto ora solo sul server “CASFILE” consentirà un monitoraggio dei software in modalità automatica. Tale implementazione fa
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.	Attualmente non implementato

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.	Gli amministratori della rete installano su ogni server e client della rete una protezione avanzata antivirus che, oltre a proteggere la macchina da virus e malware, include un servizio di classificazione automatica del 100% dei processi in esecuzione e l’analisi in tempo reale delle minacce perché controlla tutte le connessioni in uscita verso internet, l’eventuale esecuzione di un file scaricato dalla rete e l’apertura di un file allegato ad una mail. Questi file vengono verificati dalla protezione e, se appartenenti ad una lista di applicativi attendibili, si possono eseguire altrimenti vengono temporaneamente bloccati per effettuarne una verifica. Nel caso in cui non venga trovato del codice malevolo al suo interno, viene reso disponibile all’utente altrimenti viene cancellato.
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	Queste operazioni vengono svolte dall’amministratore della rete

				necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
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.	È installato presso l'ente un sistema di backup che esegue una copia dell'immagine completa di tutti i server ogni 15 minuti e le salva in un server replica. I dati dei client della rete vengono copiati giornalmente, in maniera incrementale, nel NAS di rete.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Non Applicabile
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Eventuali perdite di dati, parziali o totali, possono essere recuperate dai salvataggi automatici giornalieri che vengono eseguiti sul NAS di rete
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini dei dischi complete dei server sono memorizzate nel server replica in modo incrementale ogni 15 minuti, invece, per quanto riguarda i client, alcuni hanno l'immagine del sistema operativo memorizzata in una partizione nascosta del disco interno, per altri è presente un DVD dove c'è l'installatore del sistema Operativo: ambedue le tipologie di client hanno i dati utente memorizzati giornalmente nel NAS di rete. Tutte le immagini di backup e i dati di backup vengono replicati in modo automatico ed incrementale su un'infrastruttura esterna di replica dei dati.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Come indicato nel punto 3.3.1, le immagini sono conservate nei DVD (accessibili solo dal personale autorizzato) e nel server replica (per quanto riguarda i server) il cui accesso è protetto da password conosciuta solo dagli amministratori di rete.

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).	Per attività di gestione effettuate da reti esterne alla rete comunale vengono utilizzate connessioni VPN o comunque in SSH criptate.
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.	Attualmente non implementato
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.	Attualmente non implementato
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.	Attualmente non implementato
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Attualmente non implementato
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Attualmente non implementato
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Attualmente non implementato

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.	L' antivirus installato esegue un controllo real-time dei processi in esecuzione nella macchina ed esegue scansioni automatiche dei percorsi di sistema. Ogni client ha un agent dell'antivirus che comunica con la consolle centrale dalla quale è possibile vedere una reportistica dettagliata dei singoli client (versione dell'antivirus, aggiornamenti delle definizioni, programmi bloccati o tentativi di esecuzione). Inoltre qualsiasi tentativo di esecuzione di un programma viene prima controllato dall'antivirus per evitare di installare un malware o ransomware all'insaputa dell'utente

4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Vedi 4.1.1
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).	Funzione eseguita dalla protezione avanzata antivirus
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Log delle attività registrate nel registro antivirus dei client
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Verificabile nella console centrale dell'antivirus dove si vedono tutti i log dei client dove c'è stato un tentativo di attacco
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.	Le scansioni posso essere eseguite sia in locale, sia da remoto nella consolle centrale dove hanno accesso solo gli amministratori di rete
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.	Le scansioni possono essere eseguite su singole macchine da remoto solo da personale autorizzato

4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	La console centrale scarica gli ultimi aggiornamenti delle definizioni e li distribuisce a tutti i client della
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	Attualmente non implementato, in parte gestito dal software antivirus in collegamento continuo con i DB on line
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'applicazione delle patch di vulnerabilità è eseguita dagli Amministratori di Sistema.
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.	Attualmente non implementato in quanto non presenti sistemi separati dalla rete
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.	Attività eseguita dagli amministratori di rete
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.	Gli Amministratori di Sistema sono gli unici a verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate le patch necessarie, gli Amministratori di Sistema documentano il caso, le eventuali contromisure o la motivazione della mancata risoluzione su appositi rapportini conservato presso l'ente.
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.	Attività svolta esclusivamente dall'amministratore di rete
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.).	È stato redatto ed in fase di revisione in occasione del GDPR, il DPP (Documento Programmatico in materia di Privacy) per la gestione del rischio informatico in generale.
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.	Gli Amministratori di Sistema gestiscono la risoluzione delle vulnerabilità seguendo un livello di priorità in modo da risolvere prima le attività più 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.	Attualmente non implementato
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.	Attualmente non implementato

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.	I privilegi di amministratore sono riservati agli amministratori di sistema.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	La registrazione degli accessi degli amministratori di sistema è eseguita da un'appliance di rete che memorizza gli accessi, i warning e gli errori del controller di dominio e firma digitalmente tali log giornalmente conservando uno storico di 6 mesi.
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.	Vedi 5.1.2
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I documenti di nomina degli amministratori di sistema sono stati consegnati all'Ente.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Attualmente non implementato
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.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.

5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Funziona svolta dal log manager
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Attualmente non implementato
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Attualmente non implementato
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Funziona svolta dal log manager
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.	Attualmente non implementato

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 utenze amministrative sono composte da caratteri alfanumerici e caratteri speciali.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Il sistema di autenticazione è configurato per impedire il riutilizzo delle password precedenti per tutti gli utenti
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Il sistema di autenticazione è configurato per impedire il riutilizzo delle password precedenti per tutti gli utenti
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.	Attualmente non implementato

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.	Attualmente non implementato
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
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.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
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).	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate su un software di gestione di credenziali protetto da master password (Keepass) conosciuta solo dagli amministratori di rete.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

ABSC 8 (CSC 8): DIFESE 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.	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Tutti i PC, portatili e server Windows sono protetti da un firewall hardware installato a monte della rete

8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Attualmente non implementato
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.	La gestione dell'antivirus è eseguita dagli amministratori di rete dalla consolle centrale
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.	Dalla consolle centrale è possibile forzare l'aggiornamento e consultare il report del client
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	La protezione antivirus installata è una versione cloud: nei client è installato un agent che comunica attraverso internet con la consolle centrale
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Per l'uso di dispositivi esterni deve essere richiesta l'autorizzazione all'amministratore di rete prima di collegarlo alla rete aziendale.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Attualmente non implementato
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.	Funzioni svolte dalla protezione avanzata dell'antivirus
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Gli amministratori di sistema installano le patch rilasciate dai produttori dei sistemi operativi per correggere possibili 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.	Azione preventiva svolta dalla protezione antivirus
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Funzioni svolte dalla protezione avanzata dell'antivirus
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Funzioni svolte dalla protezione avanzata dell'antivirus
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.

8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	È stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
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.	Le mail vengono controllate da un filtro antispam e un antivirus, installati nel firewall di rete, che eseguono un controllo prima che vengano consegnate ai destinatari
8	9	2	M	Filtrare il contenuto del traffico web.	Le funzioni di content filtering sono svolte dal firewall di rete
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'antivirus installato controlla tutti gli allegati presenti nelle mail e blocca l'esecuzione di eventuali software malevoli contenuti al loro interno. Inoltre, tutti gli utenti sono stati istruiti per riconoscere le tipologie di allegati potenzialmente dannosi e come riconoscere una mail pericolosa. Se l'utente non è in grado di identificare la potenziale pericolosità di una mail, è istruito per informare tempestivamente l'amministratore di rete
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Funzioni svolte dalla protezione avanzata dell'antivirus
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.	Funzioni svolte dalla protezione avanzata dell'antivirus

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.	È installato presso l'ente un sistema di backup che esegue una copia dell'immagine completa di tutti i server ogni 15 minuti e le salva in un server replica. I dati dei client della rete vengono copiati giornalmente, in maniera incrementale, nel NAS di rete
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.	Il backup dei server include l'immagine completa del disco ogni 15 minuti. Dei client vengono copiati i dati nel NAS di rete giornalmente in maniera incrementale.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Il backup, sia dei server che dei client, viene replicato su server remoti
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Attività svolta dagli amministratori di rete
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.	Le copie dei backup vengono trasmesse ad un server remoto attraverso un canale cifrato: tale server, a sua volta, trasmette ad altri server in maniera cifrata la stessa copia del backup in modo da avere una ridondanza dei dati.
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.	Le copie dei backup effettuati sui server remoti sono allocate fisicamente all'esterno dell'ente e localizzate in sedi geografiche differenti l'una dall'altra.

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	L'analisi dei livelli particolari di riservatezza è implementata attraverso cartelle il cui accesso è regolato da specifici criteri di accesso (ACL).
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Attualmente non implementato

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.	Attualmente non implementato
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.	Attualmente non implementato
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.	Attualmente non implementato
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.	Attraverso le regole di filtri presenti nel firewall è stata creata una lista di dispositivi autorizzati ad utilizzare la rete identificandoli con l'IP della macchina. Eventuali dispositivi esterni, non presneti in questa lista, non sono autorizzati all'uso della rete
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.	Attualmente non implementato
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Attualmente non implementato
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Attualmente non implementato
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Funzioni svolte dal firewall di rete
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	Attualmente non implementato
				accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	