



**Manuale per la gestione del protocollo informatico,
dei flussi documentali e degli archivi
del Comune di Senago**

Allegato n. 13

Piano per la sicurezza informatica (Misure Minime di sicurezza)

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	L'inventario delle risorse attive è implementato utilizzando un file Excel, memorizzato all'interno di una cartella di rete, i cui accessi sono opportunamente protetti, in cui sono registrati tutti i dispositivi informatici dell'ente; Per ciascun dispositivo, sono indicate le principali caratteristiche HW e SW, L'ufficio e la persona di appartenenza e il relativo numero di inventario.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Non implementato
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	L'ente sta valutando l'acquisto di un Software dedicato.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Non implementato
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	DHCP non implementato.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	DHCP non implementato.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'inventario viene aggiornato ogni qualvolta un nuovo dispositivo viene dotato di IP e quindi collegato alla rete; Dispositivi che vengono prima approvati ed opportunamente configurati dal CED.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	L'ente sta valutando l'acquisto di un Software dedicato.
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.	L'inventario cataloga i dispositivi informatici dell'ente, secondo le seguenti informazioni. - Tipologia di Dispositivo; - Indirizzo IP; - Nome Apparato (Per la Gestione in Active Directory); - Sistema Operativo; - RAM; - Numero di Inventario - Ubicazione - Settore, Ufficio, Persona di Appartenenza Questo viene fatto per i Dispositivi quali, PC, Notebook, Stampanti, Scanner, Fax, Telefoni Digitali, Telefoni Analogici e Telefoni VoIP.

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.	Sì, L'inventario riporta tali informazioni. Non vi sono dispositivi personali collegati alla rete dell'ente.
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.	I dispositivi portatili, che elaborano e memorizzano dati di proprietà dell'ente, sono opportunamente inseriti all'interno dell'inventario.
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.	Attualmente non implementato.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Attualmente non implementato.

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.	L'elenco dei software è implementato utilizzando un file Excel, memorizzato all'interno di una cartella di rete, i cui accessi sono opportunamente protetti, in cui sono presenti i software utilizzati e le relative versioni. L'installazione dei software può essere effettuata solo dagli utenti amministratori della rete, pertanto l'installazione di ulteriori software non è consentita.
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.	La Whitelist non è implementata, tuttavia L'installazione dei software può essere effettuata solo dagli utenti amministratori della rete, pertanto l'installazione di ulteriori software non è consentita. Si sta valutando l'acquisto di Software che segnali qualora per anomalie dovessero essere presenti all'interno di un device Software non autorizzati e non inseriti nella WhiteList.
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può	Non implementata.

				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	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Non implementata.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'ente sta valutando l'acquisto di un Software dedicato.
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.	L'ente sta valutando l'acquisto di un Software dedicato.
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'ente sta valutando l'acquisto di un Software dedicato.
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.	L'ente adotta un Hypervisor utilizzato per la virtualizzazione dei server. Questo consente anche, qualora fossa necessario, di creare Macchine Virtuali destinate ad eseguire applicazioni rischiose, in ambienti isolati e protetti.

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.	Le configurazioni sicure Standard sono implementate per la protezione dei sistemi operativi.
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	La procedura di eliminazione di account non necessari, l'eliminazione di servizi non necessari e la chiusura di porte di rete aperte non utilizzate viene opportunamente seguita.

				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.	Non vengono utilizzate Immagini di installazione. Tuttavia la configurazione d'installazione software e delle sicurezza viene gestita tramite GPO.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Il servizio informatico definisce e mantiene la descrizione della configurazione standard di ogni tipologia di sistema. La descrizione è mantenuta all'intero di file word salvato in una cartella ad accesso limitato su server.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	La politica dell'ente prevede che eventuali sistemi compromessi vengano ripristinati utilizzando la configurazione standard.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Attualmente non è formalizzata alcuna procedura specifica di gestione dei cambiamenti.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Non vengono utilizzate Immagini di installazione.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Non vengono utilizzate Immagini di installazione.
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 i collegamenti da remoto vengono utilizzati i seguenti metodi: – VPN (Realizzata Mediante Firewall Watchguard) – Any Desk – Team Viewer Per i sistemi Linux viene utilizzato Secure Shell
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	Attualmente non implementato.

				sospette del sistema, delle variazioni dei permessi di file e cartelle.	
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.	Attualmente non implementato.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Attualmente non implementato.
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).	Attualmente non implementato.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Attualmente non implementato.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Attualmente non implementato.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Attualmente non implementato.
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	Attualmente non implementato.

				amministrazione.	
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.	Attualmente non implementato.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Attualmente non implementato.
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.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti sono effettuati mediante il Servizio WSUS Windows Service Update Service, nella maggior parte dei casi, mentre per determinati software vengono effettuati manualmente e periodicamente dall'amministratore di Rete.
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.
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.	Attualmente non implementato.
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.	Foglio Excel salvato su server, con accessi limitati.
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.	Non gestito.
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.).	In fase di implementazione, è previsto lo spostamento di due server che attualmente sono in LAN ed accessibili dall'esterno, questi comportano rischi per la rete LAN. Tali server sono il server di Posta Elettronica che verrà spostato all'interno di una DMZ o esternalizzato in servizio SaaS Cloud; ed il server di pubblicazione

					degli atti, Ulisse che verrà spostato in servizio SaaS Cloud.
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.	In fase di implementazione
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.	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.	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.	Esiste un elenco di utenti con i privilegi di amministratore. Tali utenze sono nominali e presentano le competenze adeguate. Gli utenti non sono amministratori locali di macchina Esiste su ogni macchina un utente amministratore locale utilizzato dal CED.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Vengono utilizzate le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, tuttavia il Log degli accessi effettuati è ancora in fase di implementazione.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Implementato ove possibile.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	In fase di implementazione.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Elenco utenti amministratori. Questo elenco viene periodicamente controllato e aggiornato, e qualora uno degli amministratori presenti nell'elenco non deve più assumere, per qualsiasi motivazione, quel ruolo, l'utenza in questione viene ridimensionata nei permessi o disabilitata.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che	Non Implementato.

				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.	All'assegnazione di nuovi client, utente Local Admin disabilitato, creazione nuovo user Admin locale con password complessa conservata secondo criteri di sicurezza.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Attualmente non Implementato.
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.	Attualmente non Implementato.
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.	L'autenticazione a due Fattori, mediante OTP, Token App, SPID viene utilizzata per tutti quei servizi in cui il sistema di riferimento ne disponga tale accesso. Esempio: - Accesso alla Console Webroot Anywhere Antivurs, l'accesso è effettuato mediante autenticazione a due 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).	Sì
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Sì
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le Credenziali delle utenze amministrative, ove possibile, vengono sostituite con frequenza mensile.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Sì
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Sì
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Attualmente non è possibile utilizzare una delle ultime 3 vecchie password per le utenze amministrative.
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	In fase di implementazione.

				privilegiato i singoli comandi.	
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.	Utenze Admin ad Hoc separate da user nominale con poteri non amministrativi.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze amministrative sono nominali, e riconducibili ad una sola persona, ed anche per quanto riguarda le utenze standard, la politica dell'ente prevede l'utilizzo di sole utenze nominative.
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.	Previsione modello accessi password cassaforte
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).	Attualmente gli accessi avvengono tramite gli Utenti Domain Admin creati appositamente
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L'ente definirà un'apposita politica di conservazione sicura delle credenziali amministrative
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Attualmente non Implementato.

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.	Installato su ogni device della rete il software Webroot Secure Endpoint.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	- Webroot - Windows Firewall (non attivo, o attivo con restrizioni) su tutti gli

					Endpoint.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Repository di Endpoint presente.
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.	Attivo con blocco lato utente.
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.	Si è presente la console di gestione centrale offerta da Webroot, accessibile da Internet, mediante autenticazione a due fattori.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Attualmente non implementato.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'ente predilige l'uso dei propri dispositivi; in casi eccezionali, dopo gli opportuni controlli, consente l'uso di quelli esterni e definisce che questo deve essere limitato alle sole attività aziendali
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	L'ente sta valutando l'acquisto di un Software dedicato.
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.	Attualmente non implementato.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Attualmente non implementato.
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.	Attualmente non implementato.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Attualmente non implementato.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Effettuato tramite HTTP/HTTPS Proxy Policy da Firewall Watchguard.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	In fase di implementazione.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Esecuzione automatica dei contenuti dinamici, quali macro, disattivata
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Apertura automatica disattivata

8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Anteprima automatica disattivata
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	In valutazione.
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.	Effettuato tramite Firewall Watchguard
8	9	2	M	Filtrare il contenuto del traffico web.	Effettuato tramite Firewall Watchguard
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).	Effettuato tramite Firewall Watchguard
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Attualmente non implementato.
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.	Attualmente non implementato.

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.	Copia di sicurezza effettuata settimanalmente, con Veeam Backup.
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.	Veeam Backup Service.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Attualmente non Implementato..
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Il ripristino di prova viene periodicamente effettuato su singoli file.
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	In fase di implementazione

				nel cloud.	
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.	Copie di backup del sistema vengono memorizzate su supporti fisici HDD settimanalmente, questi non sono accessibili dalla rete, e vengono conservati in un apposita cassetta di sicurezza anti-fuoco.

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	Da verificare coi responsabili di settore.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Segue la 13.1.1.
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 gestito.
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 gestito.
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 gestito.
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.	Attualmente non gestito.
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	Attualmente non gestito.

				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.	Attualmente non gestito.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Attualmente non gestito.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Effettuato tramite Firewall Watchguard
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.	Attualmente non gestito.