

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	PARZIALMENTE IMPLEMENTATO SERVER locale - Inventario disponibile PC – Inventario disponibile Apparati mobili (PC portatili, tablet) – Non vi sono apparati mobili Gli inventari saranno richiesti alla ditta manutentrice (attualmente CNR Service S.r.l.), in funzione della disponibilità di risorse economiche.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	NON IMPLEMENTATO nella fase attuale
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	NON IMPLEMENTATO nella fase attuale
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	NON IMPLEMENTATO nella fase attuale
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	PARZIALMENTE IMPLEMENTATO Procedura standard a cura della ditta manutentrice (CNR Service) in fase di implementazione.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	NON IMPLEMENTATO nella fase attuale
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	PARZIALMENTE IMPLEMENTATO Incluso nel punto 1.1.1.

				IP.	
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.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	NON IMPLEMENTATO nella fase attuale

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.	PARZIALMENTE IMPLEMENTATO Server – sw autorizzati gestiti direttamente dall'Amministratore di Rete (attualmente coincidente con Siscom e Technical Design.) Gli Applicativi gestionali sono installati e gestiti dai fornitori Siscom e Technical Design Gli applicati di office automation sono installati dal fornitore (CNR Service) È intenzione dell'Amministrazione procedere in tempi ragionevoli

					alla definizione di nuove policy che verosimilmente toglieranno detti privilegi agli Utenti senza le adeguate competenza.
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 IMPLEMENTATO nella fase attuale
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).	NON IMPLEMENTATO nella fase attuale
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	NON IMPLEMENTATO nella fase attuale
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	NON IMPLEMENTATO Controlli periodici manuali potranno essere richiesti al fornitore in funzione della disponibilità di risorse economiche.
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.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
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	NON IMPLEMENTATO nella fase attuale

				essere installate in ambienti direttamente collegati in rete.	
--	--	--	--	---	--

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PARZIALMENTE IMPLEMENTATO SERVER: La manutenzione dei server è a chiamata ed il fornitore non può garantire la configurazione. Il Servizio da "Amministratore di Sistema" permette di avvicinarsi ad una gestione controllata e sarà implementato dall'Amministrazione in funzione della disponibilità di risorse economiche. PC: configurati per gli aggiornamenti automatici
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.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	IMPLEMENTATO Il fornitore CNR Service utilizza configurazioni standard
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	IMPLEMENTATO Vedi punto 3.2.1.

3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	NON IMPLEMENTATO nella fase attuale
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	PARZIALMENTE IMPLEMENTATO Non sono utilizzate immagini di installazione, ma i sw da installare sono conservati off line
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	NON IMPLEMENTATO nella fase attuale
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).	IMPLEMENTATO SERVER, APPARATI DI RETE e PC sono mantenuti solo "in loco". Applicativi gestionali sono mantenuti remotamente con sw di teleassistenza la cui sicurezza è garantita dal fornitore (Siscom e Technical Design)
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.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	NON IMPLEMENTATO nella fase attuale
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	NON IMPLEMENTATO nella fase attuale

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.	NON IMPLEMENTATO È utilizzato il sistema di sicurezza ESET NOD 32 e un modello di firewall costituito da un firewall di rete più firewall locale. L'Amministrazione riconosce la disponibilità di altri strumenti automatici più articolati per la ricerca di vulnerabilità e si impegna ad applicarli in funzione della disponibilità di risorse economiche.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	NON IMPLEMENTATO nella fase attuale

4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità.	NON IMPLEMENTATO nella fase attuale
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	NON IMPLEMENTATO Vedi punto 4.1.1. L'antivirus è configurato per aggiornamento automatico
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	NON IMPLEMENTATO nella fase attuale
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	IMPLEMENTATO PC: Il Sistema operativo e le applicazioni di office automation delle postazioni di lavoro sono aggiornate tramite aggiornamenti automatici di Microsoft. SERVER: Le installazioni sono a cura del fornitore (Siscom e Technical Design)
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in	NON APPLICABILE

				particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	
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 IMPLEMENTATO nella fase attuale
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.	IMPLEMENTATO PARZIALMENTE L'antivirus è aggiornato automaticamente. Il Firewall è aggiornato su richiesta. Il Servizio da "Amministratore di Sistema" permette di avvicinarsi ad una gestione controllata e sarà implementato dall'Amministrazione, in funzione della disponibilità di risorse economiche.
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 IMPLEMENTATO nella fase attuale
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.).	NON IMPLEMENTATO Manca azione
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.	PARZIALMENTE IMPLEMENTATO Tutte le patch sono applicate in tempo reale per antivirus, sistemi operativi, office automation. I sw gestionali e firewall manuale a cura dei fornitori non in tempo reale
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 nella fase attuale

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 nella fase attuale

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.	NON IMPLEMENTATO Al fine di garantire la continuità dei servizi, attualmente gli Utenti hanno privilegi da Amministratore del PdL. È intenzione dell'Amministrazione procedere in tempi ragionevoli alla definizione di nuove policy che verosimilmente toglieranno detti privilegi agli Utenti senza le adeguate competenza.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	NON IMPLEMENTATO È intenzione dell'Amministrazione implementare il log accessi di Microsoft e dipendentemente dalla disponibilità economica, la sua conservazione per un periodo adeguato.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	NON IMPLEMENTATO nella fase attuale
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	NON IMPLEMENTATO nella fase attuale
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	NON IMPLEMENTATO SERVER - Chiedere all'Amministrazione (o Società MAC PAL) se l'elenco è disponibile. Gestionali – gestiti da fornitore Siscom e Technical Design (elenco Amministratori) PdL – Chiedere all'Amministrazione (o Società MAC PAL) se l'elenco è disponibile.

5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	NON IMPLEMENTATO nella fase attuale
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.	PARZIALMENTE IMPLEMENTATO Procedura standard a cura della ditta manuttrice (attualmente CNR Service). Nota: Essendo il contratto con CNR Service non esclusivo non c'è la garanzia che ciò avvenga sempre.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	NON IMPLEMENTATO nella fase attuale
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	NON IMPLEMENTATO nella fase attuale
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	NON IMPLEMENTATO nella fase attuale
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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).	IMPLEMENTATO
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	NON IMPLEMENTATO nella fase attuale

5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	NON IMPLEMENTATO
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	NON IMPLEMENTATO
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	NON IMPLEMENTATO nella fase attuale
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	IMPLEMENTATO
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	IMPLEMENTATO
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.	IMPLEMENTATO

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).	NON IMPLEMENTATO nella fase attuale
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	IMPLEMENTATO
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	NON APPLICABILE Non vengono utilizzati certificati

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.	IMPLEMENTATO Attraverso la piattaforma ESET NOD 32
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	IMPLEMENTATO Tutti i PC sono protetti da firewall locale e IPS personale, implementato in ESET NOD 32.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale

8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	NON IMPLEMENTATO nella fase attuale
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PARZIALMENTE IMPLEMENTATA L'Amministrazione definirà una policy adeguata sull'uso degli Strumenti aziendali
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	NON IMPLEMENTATO nella fase attuale
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	NON IMPLEMENTATO nella fase attuale.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	IMPLEMENTATO
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	NON IMPLEMENTATO Reso necessario dall'applicativo gestionale Siscom
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta	NON IMPLEMENTATO

				elettronica.	L'Amministrazione valuterà la disattivazione.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	IMPLEMENTATO Da verificare
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	NON IMPLEMENTATO L'Amministrazione valuterà la disattivazione.
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.	IMPLEMENTATO La posta aziendale viene protetta dalle procedure del fornitore provider (Siscom - verificare)
8	9	2	M	Filtrare il contenuto del traffico web.	NON IMPLEMENTATO L'Amministrazione valuterà l'introduzione di policy di filtraggio.
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).	IMPLEMENTATO Attraverso le funzionalità standard di MS-outlook
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale

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.	IMPLEMENTATO PC Come policy aziendale è data indicazione che i file di lavoro devono

					essere salvati su gli share di rete. Per cui non viene eseguito il backup dei singoli PC. SERVER Il backup è effettuato giornalmente.
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.	NON IMPLEMENTATO nella fase attuale
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	NON IMPLEMENTATO nella fase attuale
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	NON IMPLEMENTATO nella fase attuale
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.	IMPLEMENTATO Le cassette di backup sono conservate in appositi armadi protetti.
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.	IMPLEMENTATO Incluso nel punto 10.3.1

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 IMPLEMENTATO L'Amministrazione effettuerà l'analisi con il supporto delle Società fornitrici, in funzione della disponibilità di risorse economiche.

13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	NON IMPLEMENTATO nella fase attuale
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 exfiltrazione di informazioni.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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 IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
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.	NON IMPLEMENTATO nella fase attuale
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	NON IMPLEMENTATO nella fase attuale
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	NON IMPLEMENTATO nella fase attuale

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	NON IMPLEMENTATO L'Amministrazione valuterà l'introduzione di policy di filtraggio.
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.	NON IMPLEMENTATO nella fase attuale