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	È a disposizione uno strumento software che permette di individuare tutti i dispositivi collegati alla rete identificandoli per: - indirizzo IP - nome del dispositivo - tipologia di servizi offerti.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Lo strumento automatico di rilevazione verrà attivato nel secondo semestre del 2021 compatibilmente con le risorse economiche disponibili.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Vedi 1.1.2
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	È stato implementato un sistema di rilevazione del traffico dei dispositivi con contestuale analisi del traffico anomalo.
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	IL log del server DHCP è attivo.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento dell'inventario viene svolto con cadenza mensile e comunque ogni volta che viene aggiunta una o più risorse informatiche.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Vedi 1.1.2
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.	È a disposizione uno strumento software che permette di individuare tutti i dispositivi collegati alla rete identificandoli per: - indirizzo IP - nome del dispositivo - tipologia di servizi offerti.
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	Queste informazioni sono presenti nello strumento software a disposizione.

				informazioni sul fatto che il dispositivo sia portatile e/o personale.	
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.	Da implementare nel primo semestre 2022

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.	Il nostro personale dispone di una tabella concordata con il responsabile della struttura relativamente ai programmi utilizzati. Attraverso operazioni di formazione aziendale gli utenti sono stati sensibilizzati sull'utilizzo dei programmi e dei rischi che si corrono con software non autorizzato.
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.	Ne è previsto lo studio nel secondo semestre 2021, con eventuale implementazione nel primo semestre 2022 compatibilmente con le risorse economiche disponibili.
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).	Vedi 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.	Vedi 2.2.1
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Durante le normali operazioni di manutenzione i tecnici verificano la conformità del software installato. Complessivamente i nostri operatori non hanno la dimestichezza e le conoscenze per installare software in autonomia.

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.	Vedi 1.1.2
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.	Vedi 1.1.2

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.	I tecnici che si occupano della manutenzione hanno a disposizione una procedura standard di installazione. Le configurazioni applicate prevedo le seguenti operazioni standard di sicurezza minima: - aggiornare il sistema operativo con le ultime versioni; - installare subito il sistema antivirus/antimalware; - attivare le funzioni di firewall e IPS sul client; - rimuovere gli accessi di tipo GUEST.
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.	Vedi 3.1.1
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	I tecnici che si occupano della manutenzione hanno a disposizione una procedura standard di installazione. Le configurazioni applicate prevedo le seguenti operazioni standard di sicurezza

					minima: - aggiornare il sistema operativo con le ultime versioni; - installare subito il sistema antivirus/antimalware; - attivare le funzioni di firewall e IPS sul client; - rimuovere gli accessi di tipo GUEST. Un elemento migliorativo già in parte sviluppato di cui è previsto il completamento nel primo semestre 2022 è quello di preparare un'immagine standard di installazione per i pc client.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Qualora i sistemi client vengano compromessi a causa di malware la direttiva tecnica è quella di ripristinare da zero l'installazione eseguendo la formattazione a basso livello del disco, o la sostituzione del disco stesso.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	E' presente una check list di installazione
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	E' stato impostato, ma verrà ulteriormente sviluppata una serie di immagini MEMORIZZATE SU SUPPORTI ESTERNI AL SISTEMA per il ripristino delle configurazioni standard.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Le immagini di installazione sono memorizzate su supporti separati non raggiungibili dalla 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).	Le connessioni di amministrazione da remoto dei tecnici vengono eseguite attraverso strumenti che usano canali sicuri. Nello specifico il programma utilizzato consente la triangolazione con un server sicuro di connessione. Sono inoltre state implementate connessioni esterne sicure.

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.	I tecnici che eseguono le installazioni si tengono continuamente aggiornati sulle eventuali vulnerabilità dei sistemi. In caso di installazione montano sempre le ultime versioni stabili ed aggiornate contro le possibili e note vulnerabilità.
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	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il sistema di antivirus / antimalware gestisce anche i possibili attacchi di vulnerabilità in quanto esamina i processi in esecuzione sul sistema e li confronta sia con un archivio interno che con un archivio via cloud di possibili minacce.
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	Il servizio indicato è attivo nel sistema antivirus installato.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	E' attivo un sistema di aggiornamento automatico dei sistemi operativi. Periodicamente viene controllato che non si sia disattivato.
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.	In generale non abbiamo questa situazione in quanto i dispositivi sono sempre agganciati alla 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.	La funzione richiesta è presente e monitorata dalla console centralizzata del sistema antivirus.
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.	In caso di vulnerabilità rilevate su strumenti datati, vengono installate le ultime versioni di patch. Tutta la macchina viene verificata con gli strumenti antivirus/antimalware per verificare la possibile presenza di tracce residue. In caso di incertezze, il sistema viene ricaricato con l'installazione standard.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei	E' presente un documento che cataloga tutti i sistemi

				livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	potenzialmente esposti a minacce esterne. Molti dei possibili sistemi raggiungibili in esterno sono gestiti tuttavia in esterno come - mail server - webserver
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.	Vedi 4.1.1
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Le patch proposte dagli aggiornamenti di sistema prima di essere applicate vengono provate dei nostri responsabili CED.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Le credenziali di amministrazione sono in possesso ai soli tecnici della manutenzione ed alla referente interno e responsabile amministrativo.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'utilizzo delle credenziali amministrative viene fatto solo per operazioni sui server o sui dispositivi di controllo della funzionalità delle rete. L'utilizzo di tali credenziali viene registrato dai log di sistema e da quello dei dispositivi.
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.	Sono memorizzate all'interno dei log di sistema
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	È presente un registro di assegnazione delle credenziali amministrative e la data di assegnazione.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le	Quando viene collegato un nuovo dispositivo, tipicamente un PC,

				credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	vengono rimosse tutte le credenziali di accesso di default ed utenti tipo Guest.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Questa funzione viene gestita tramite un opportuno registro gestito dal responsabile CED.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Sono memorizzate all'interno dei log di sistema
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 credenziali di tipo amministrativo si attengono a quanto indicato.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le credenziali di tipo amministrativo si attengono a quanto indicato.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le credenziali di utenze amministrative vengono cambiate ogni 6 mesi.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Questa funzione è gestita a livello di policy del sistema operativo di rete.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Questa funzione è gestita a livello di policy del sistema operativo di rete.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Questa funzione è gestita a livello di policy del sistema operativo di rete.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Si conferma questa richiesta.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	È presente un registro di assegnazione delle credenziali amministrative e la data di assegnazione.
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.	Le utenze di "root" e "Administrator" vengono utilizzate solo per attività speciali di installazione. Per il monitoraggio e la normale gestione sono usati utenti con credenziali ammnistrative ed assegnate in modo individuale.

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L'elenco delle credenziali è disponibile sia per il responsabile ced che per quello amministrativo.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si usano certificati digitali.

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 della rete è installato un sistema antivirus e anti malware aggiornato in automatico e con bassissima latenza di aggiornamento in caso di diffusione massiva di malware.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Lo strumento utilizzato di cui al punto sopra al al suo interno un sistema Firewall e IPS.
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.	Questa funzione è presente nel sistema di gestione centralizzato
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Questa funzione è presente nel sistema di gestione centralizzato
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Gli operatori sono stati opportunamente istruiti per l'utilizzo dei sistemi esterni quali chiavette, hard disk e simili. AZIONI FUTURE: Verrà organizzato nel secondo semestre 2021 un'azione di follow-up di aggiornamento su questa materia.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	È allo studio questa funzione
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento	Il sistema antivirus utilizzato è già predisposto per bloccare

				della connessione dei dispositivi removibili.	eventuali processi malevoli che si attivano alla connessione dei supporti mobili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	La funzionalità di esecuzione automatica dei contenuti dinamici è disattivata.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il sistema antivirus utilizzato è già predisposto per bloccare eventuali processi malevoli che si innescano dalle aperture delle e-mail in modalità anteprima.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	La funzionalità di anteprima dei contenuti dei file è disattivata.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Il sistema antivirus presente è in grado di verificare se i dispositivi esterni eseguono dei processi malevoli e nel caso di bloccarli.
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.	Il sistema di Antispam utilizzato a livello di provider permette di gestire questa funzionalità.
8	9	2	M	Filtrare il contenuto del traffico web.	E' presente un firewall che svolge una verifica dei contenuti.
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).	Nella posta elettronica i contenuti malevoli sono bloccati a livello di provider. Per la parte web è stata potenziata la gestione di accesso alle diverse tipologie di contenuto.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Il sistema antivirus e anti malware svolge la funzione richiesta.
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.	Il sistema antivirus e anti malware svolge la funzione richiesta.

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.	Il sistema di backup prevede una copia delle intere macchine virtuali con una 'retention' di 30 giorni. Tutti i file sono salvati in sistemi NAS con credenziali di accesso utilizzate solo dai sistemi di backup e diverse da quelle standard.
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 sistema di backup prevede una copia delle intere macchine virtuali con una 'retention' di 30 giorni. Tutti i file sono salvati in sistemi NAS con credenziali di accesso utilizzate solo dai sistemi di backup e diverse da quelle standard.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Il backup viene svolto sia con copie di intere macchine virtuali che di singoli file.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Il sistema di copia delle macchine virtuale esegue settimanalmente una verifica di consistenza dell'eventuale ripristino.
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 di sicurezza sono cifrate grazie alla sicurezza intrinseca ai sistemi NAS utilizzati. I dati sono ulteriormente criptati.
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 di backup non hanno privilegi di accesso direttamente raggiungibili dal sistema operativo.

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	Sono presenti i profili di autorizzazione che gestiscono le informazioni riservate.

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.	Sono funzioni che vengono svolte dal firewall in dotazione alla struttura. Come aggiornamento rispetto all'edizione iniziale delle Misure Minime di sicurezza, i nostri tecnici hanno previsto anche tutte le modalità di collegamento sicuro per le tipologie di operatori che lavorano in smart-working e/o lavoro agile. Ogni utente ha un proprio set di credenziali per accedere dall'esterno.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il sistema antivirus utilizzato è già predisposto per bloccare eventuale traffico anomalo verso url presenti in black-list. Inoltre il firewall è impostato per bloccare siti e/o risorse esterne presenti nelle blacklist