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 Dotazioni val Brembilla.xlsx è riportato in allegato al presente documento nel file Allegato 4.2 – Misure Complete.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'inventario di cui alla misura 1.1.1 è aggiornato manualmente in Excel ed estrapolato in automazione da Logmein Central.
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.	Con scansione su rete. Vedi punto 1.1.1

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.	Elenco software autorizzati e non da pannello in cloud antivirus WithSecure elements Installazione software sui client solo dagli amministratori.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Scansioni effettuate in automazione da antivirus WithSecure elements.

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.	Sono state definite e documentate le configurazioni sicure standard per la protezione dei sistemi operativi utilizzati.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Configurazioni standard uniformate.

3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Gli eventuali sistemi in esercizio che vengono compromessi vengono ripristinati e configurati in modo standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Immagini d'installazione memorizzate offline su NAS.
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).	L'accesso remoto viene loggato ed effettuato con Logmein.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Il controllo mediante Logmein Central scansiona i software installati e genera report sulle eventuali vulnerabilità di sicurezza sulle patch di aggiornamento mancanti.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Le definizioni dell'antivirus vengono aggiornate automaticamente dal pannello centralizzato in cloud e poi rimandate ai vari client. Per gli aggiornamenti dei software mediante Logmein central le patch sono verificate dal portale stesso.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Le patch e gli aggiornamenti vengono scaricati e installati automaticamente.
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.	Vengono periodicamente aggiornati manualmente i sistemi non raggiungibili via 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.	Viene verificato che le vulnerabilità emerse dalle scansioni siano state risolte per mezzo di patch o manualmente.
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.).	Misura non implementata.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare	Viene attribuita la priorità alle patch evolutive dei sistemi operativi server e client.

				applicare le patch per le vulnerabilità a partire da quelle più critiche.	

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 espressamente nominati da parte dell'ente.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	È attivato il log di sistema per registrare gli accessi come amministratore su PC, server, apparati di rete.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	E' presente la lista delle utenze amministrative e delle altre con garanzia che sono autorizzate.
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.	Vengono sostituite le credenziali dell'amministratore predefinito prima di collegare alla rete un nuovo dispositivo.
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).	Per le utenze amministrative vengono utilizzate credenziali complesse con simboli e caratteri alfanumerici.
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 ultime 4 password per tutti gli utenti.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Vengono distinte le utenze amministrative e non con credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze sono riconducibili a una sola persona.
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	Le utenze amministrative anonime sono utilizzate solo per emergenza e riconducibili a chi le ha utilizzate.

				essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Vengono conservate le credenziali amministrative.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Dove vengono utilizzati certificati digitali le chiavi sono protette.

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 sistemi connessi alla rete è installato l'antivirus locale WithSecure elements con pannello centrale in cloud per la gestione e distribuzione degli aggiornamenti in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	L'antivirus WithSecure elements contiene la gestione del firewall al suo interno.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	È stata data disposizione di limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'apertura automatica dei dispositivi rimovibili è disattivata.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'apertura automatica di contenuti esterni nei file è disattivata.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'apertura automatica delle e-mail è disattivata.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	L'anteprima dei file è disattivata.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'antivirus su pc esegue automaticamente la scansione degli eventuali dispositivi connessi prima di poterli utilizzare.
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.	Antispam in cloud con utilizzo di Exchange Online.
8	9	2	M	Filtrare il contenuto del traffico web.	Content filter configurato su firewall per filtrare il contenuto.
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).	I file non idonei vengono controllati dall'antispam in cloud per la posta elettronica e dal firewall per il traffico web.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Giornalmente vengono effettuati i backup.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	I backup vengono cifrati in automazione dal software.
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.	In locale le copie sono accessibili solo da utenti amministrativi e in cloud le copie sono permanentemente scollegate dal sistema.

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	Funzione attualmente non implementata.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il traffico da e verso url viene bloccato dal firewall con blacklist e whitelist.