

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	Per quanto riguarda le risorse di rete collegate alle reti Wi-Fi MasterCom questo viene effettuato automaticamente dal firewall centralizzato. Sono stati rilevati i dispositivi attivi sulla rete di segreteria mediante scanner di rete alla accensione di tutte le macchine. Lo stesso per quanto riguarda la rete dei laboratori e aule speciali.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Come punto ABSC 1.1.1 per quanto riguarda la rete Wi-Fi
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato in modo automatico dal firewall centralizzato per la gestione della rete Wi-Fi, per ciò che riguarda allarmi su anomalie è necessario definire in modo più stretto cosa si intende per anomalie onde evitare il classico problema degli eccessivi falsi positivi.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato in modo automatico dal firewall centralizzato per la gestione della rete Wi-Fi
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Per il server DHCP attivato sulle reti Wi-Fi MasterCom questo viene effettuato dal firewall centralizzato per la gestione della rete Wi-Fi
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato in modo automatico dal firewall centralizzato per la gestione della rete Wi-Fi è possibile ovviamente in più utilizzare tale "logging" autonomamente per affinare ulteriormente tale elenco
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato dal firewall centralizzato per la gestione della rete Wi-Fi in concomitanza con il server MasterCom Alla attivazione dei nuovi dispositivi questi vengono aggiunti all'inventario sulla rete di segreteria e dei laboratori.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato dal firewall centralizzato per la gestione della rete Wi-Fi in concomitanza con il server MasterCom e il controller rete Wi-Fi

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.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato dal firewall centralizzato per la gestione della rete Wi-Fi La rete di segreteria e dei laboratori è basata su dhcp, l'indirizzo IP è quindi variabile. Si provvede a registrare il mac della macchina.
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.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom viene effettuato dal firewall centralizzato per la gestione della rete Wi-Fi in concomitanza con il server MasterCom
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.	
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.	Per le reti Wi-Fi MasterCom esiste la possibilità di implementazione di questo obiettivo tramite controller Wi-Fi. Necessario prevedere server RADIUS per autorizzazione 802.1.X
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

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.	Per ciò che concerne qualunque server MasterCom esiste è presente e costantemente aggiornato tale elenco. È stato stilato l'elenco dei software installati sulla rete di segreteria e dei laboratori. Nei pc solo gli amministratori possono installare programmi
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.	Per ciò che concerne qualunque server MasterCom vale quanto detto al punto ABSC 2.1.1

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).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Su tutti i server MasterCom vengono regolarmente effettuate tali scansioni al rilascio di ogni nuova versione del software. Il controllo viene effettuato dagli amministratori e, quando possibile in rete con programmi predisposti sulla rete di segreteria e dei laboratori.
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.	
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.	
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.	

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.	Tutti i server MasterCom utilizzano configurazioni sicure standard. Sulla rete di segreteria e dei laboratori i sistemi operativi sono stati installati la prima volta con configurazione standard prevista dal dispositivo. Successive installazioni vengono fatte a partire dal sistema operativo originale.

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.	Le configurazioni sicure standard dei server MasterCom corrispondono nativamente alle versioni "hardened"
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.	Tutte le immagini dei server MasterCom vengono regolarmente aggiornate con le più recenti patch di sicurezza.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Per i server MasterCom sono già predefinite ed obbligate dal sistema stesso E' stata definita la configurazione standard per i dispositivi suddivisi per sistema operativo e per applicativi installati sulla rete di segreteria e dei laboratori.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Per i server MasterCom è quello che avviene normalmente E' conservata copia della configurazione standard e i dispositivi vengono ripristinati a partire da tale configurazione per la rete di segreteria e dei laboratori..
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione dei server MasterCom sono memorizzate anche offline Le immagini di installazione vengono conservate su chiavi usb per la rete di segreteria e dei laboratori.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
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).	Tutte le operazioni di amministrazione remota relative ai server MasterCom avvengono in modalità protetta tramite canale SSH e con certificati personali Le operazioni di amministrazione remota vengono effettuate su protocollo https per la rete di segreteria e dei laboratori.

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.	Per i server MasterCom vedere punto ABSC 2.3.1
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.	Per i server MasterCom è quello che avviene normalmente
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.	Per tutto il software MasterCom è quello che avviene nella gestione ordinaria
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni 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.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

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.	Da implementare con la installazione di scanner di rete per la scansione e ricerca delle vulnerabilità
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
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).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eeguire 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.	
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.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Da implementare Il software di rete prescelto verrà aggiornato automaticamente alle nuove versioni
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	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Tutti i server MasterCom e i relativi software hanno come impostazione di base l'aggiornamento automatico di tutte le patch di sicurezza di qualunque tipo Tutti i computer sono predisposti per l'aggiornamento automatico per il sistema operativo e per le applicazioni per la rete di segreteria e dei laboratori.
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.	Non implementabile attualmente e non necessario per assenza di tali apparati.

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.	
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 redatto un registro delle vulnerabilità emerse e delle modalità di trattamento
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.	
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.).	Viene redatto un registro delle vulnerabilità emerse e delle modalità di trattamento
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.	Viene definito un piano di gestione dei rischi e vulnerabilità e delle modalità di trattamento. Punto 471
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.	
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.	

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.	Tutti i sistemi MasterCom e i relativi server sono gestiti direttamente dalla MasterTraining con i propri tecnici qualificati ed identificati.

					Sono stati individuati agli amministratori dei sistemi in rete dotati di adeguate competenze per la rete di segreteria e dei laboratori.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Ogni accesso di un'utenza amministrativa ad un server MasterCom viene automaticamente registrato nei vari log previsti. Viene redatto un registro degli interventi degli amministratori sui diversi dispositivi per la rete di segreteria e dei laboratori
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Tutti i sistemi MasterCom prevedono l'utilizzo di questa best practice
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Tutti i sistemi MasterCom e i relativi server hanno le proprie ACL. E' stato creato un registro delle utenze amministrative per la rete di segreteria e dei laboratori
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che 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.	Alla attivazione dei nuovi dispositivi si provvede a creare l'utente amministratore
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa	Nei log vengono regolarmente tracciate tutte le modifiche alle utenze amministrative del sistema MasterCom
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Nel sistema MasterCom tramite i propri log vengono regolarmente tracciati tutti gli accessi di tutte le utenze amministrative e non
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.	

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).	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto. Si sono utilizzate credenziali conformi
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto. E' stata stabilita una scadenza password semestrale
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto. Si mantiene registro delle utenze e relative password
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto.
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.	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto.
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.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto. Tutti i dispositivi attivi prevedono l'utente standard e l'amministratore
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Il sistema MasterCom incoraggia questa best practice ma la sua applicazione è lasciata all'Istituto. Le password di tutti gli utenti sono personali
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'immutabilità di chi ne fa uso.	Per tutti i server MasterCom le credenziali amministrative anonime del sistema quale "root" (in questo caso di LINUX) non vengono mai utilizzate se non in casi di disaster recovery in cui non è possibile utilizzare quelle nominative. Ciò vale anche per la rete di segreteria e dei laboratori.

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).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Si mantiene registro delle utenze e relative password
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Per accedere ai server MasterCom come amministratori si accede sempre con un sistema a chiavi pubblica e privata e tutte le chiavi private di ogni utente autorizzato sono adeguatamente protette dai sistemi previsti dall'azienda. Per la rete di segreteria e dei laboratori non è previsto l'uso di 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.	Tutti i pc sono dotati di antivirus antimalware standard, windows defender aggiornati automaticamente
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Ogni server MasterCom è dotato del proprio firewall dedicato interno Per la rete di segreteria e dei laboratori tutti i pc sono dotati di firewall standard di windows.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
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.	
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.	

8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Tutti gli utenti sono stati avvisati della necessità
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
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.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
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.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	implementata
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	implementata
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	implementata
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	implementata
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	implementata
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.	Secondo client di posta utilizzato o gestore posta web
8	9	2	M	Filtrare il contenuto del traffico web.	Il traffico web viene filtrato attraverso firewall
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).	Non implementabile attualmente

8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
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.	

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.	La copia dei dati del sistema MasterCom Pro avviene in tempo reale su server dislocati geograficamente in luoghi differenti, inoltre viene fatta una "fotografia storicizzata" di tali dati ogni giorno. Tutti gli altri server MasterCom hanno backup quotidiani di tutti i dati necessari al ripristino completo del sistema. Per la rete di segreteria e dei laboratori viene fatto un backup dei dati necessari ogni giorno
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.	Tutti i server MasterCom mettono in atto tutti i backup necessari a soddisfare tale punto
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Vedi punto ABSC 10.1.1
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Le procedure generali di ripristino dei server MasterCom vengono verificate ogni settimana
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.	Tutti i dati ritenuti sensibili dei server MasterCom sono cifrati prima di essere trasferiti ai repository di backup Per la rete di segreteria e dei laboratori Implementata anche con remotizzazione del backup
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Le copie dei dati dei server MasterCom vengono mantenute su 3 differenti data center dislocati su reti geografiche differenti.

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	Tutti i dati ritenuti rilevanti dei server MasterCom sono cifrati prima di essere trasferiti ai repository di backup Per la rete di segreteria e dei laboratori Implementata anche con remotizzazione del backup
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
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.	Per dispositivi che si collegano alle reti Wi-Fi MasterCom c'è la possibilità di gestione specifica, secondo richieste dell'Istituto, tramite firewall centralizzato di bloccare porte specifiche sulla rete Wi-Fi (esempio abilitare solo la 443 ssl)
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.	
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.	
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.	
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.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Per i dispositivi che si collegano alle reti Wi-Fi MasterCom il traffico in uscita e in entrata viene registrato tramite firewall centralizzato. Possibilità di consultazione ed esportazione dei log.

13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Per i dispositivi che si collegano alle reti Wi-Fi MasterCom il traffico in uscita viene monitorato da un sistema di controllo. Il traffico può essere analizzato tramite diversi filtri.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Per i dispositivi che si collegano alle reti Wi-Fi MasterCom questo è effettuato da firewall centralizzato. Le blacklist vengono regolarmente scaricate quotidianamente. Possibilità di personalizzare blacklist e whitelist manualmente. Per la rete di segreteria e dei laboratori Implementata mediante firewall.
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.	