



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

Allegato n. 13

Piano di sicurezza (Misure Minime ICT)

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario delle risorse attive è in fase di aggiornamento rispetto agli ultimi acquisti e si trova in \\srv18\CED\inventario Attualmente l'inventario è gestito in maniera manuale ma è in fase di attivazione il sistema Spiceworks che permette di automatizzarle il mantenimento.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	L'inventario attualmente è implementato attraverso azioni manuali, ma è in fase di attivazione il sistema Spiceworks che permetterà di effettuare una gestione automatizzata dello stesso
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Il discovery dei dispositivi è in fase di implementazione tramite il sistema Spiceworks. I risultati del discovery verranno analizzati dal servizio informatico per valutare eventuali anomalie e definire verifiche o aggiornamenti dell'inventario.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Non son attualmente attivi sistemi di analisi del traffico interno di rete
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Log di Windows
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Periodicamente vengono effettuati controlli manuali
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	I nuovi dispositivi vengono preparati e approvati dal Ced. In seguito il Ced inserisce il nuovo dispositivo nell'inventario con le relative caratteristiche ed infine lo collega alla rete
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	I dispositivi collegati alla rete approvati sono già inseriti in inventario prima del collegamento alla rete. Lo strumento di discovery automatica Spiceworks verrà utilizzato per avere le informazioni su cui effettuare analisi e definire gli eventuali inserimenti/modifiche da effettuare manualmente sull'inventario.

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.	All'interno dell'inventario vengono registrate le seguenti informazioni: <u>Personal computer</u> : sistema operativo, cpu, ram, hard disk, numero di serie, anno di acquisto, settore/ufficio e assegnatario, IP. <u>Server</u> : tipo (fisico/virtuale), indirizzo ip, nome server, ubicazione <u>Stampanti e ed altri device</u> : ufficio, marca, modello, tipo, assegnatario, indirizzo IP (dove presente) <u>Apparti di rete/firewall</u> : tipo, indirizzo ip, ubicazione
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 tutti i dispositivi che possiedono un indirizzo IP l'inventario indica il nome della macchina, la funzione, un titolare responsabile e l'ufficio associato. Inoltre per ogni tipologia di attrezzatura l'inventario riporta le specifiche informazioni caratteristiche. (es. per i client RAM, HD, MAC address etc.)
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.	Al momento telefoni cellulari e tablet non sono censiti. Le restanti attrezzature sono già inventariate
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Attualmente l'autenticazione a livello 802.1 non è implementata
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Per le connessioni alla rete locale non vengono utilizzati certificati lato cliente

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	Da implementare \\srv18\CED\software

				consentire l'installazione di software non compreso nell'elenco.	
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.	Attualmente non sono implementate specifiche "whitelist" o blocchi automatici di esecuzione di software non incluso nella lista. L'installazione dei software sui sistemi può essere effettuata solo dal servizio Ced in quanto gli altri utenti non hanno profili di accesso ai sistemi con privilegi di amministratore.
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).	Attualmente questa casistica non è gestita
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Non vengono attualmente effettuate verifiche di integrità dei file relativi alle applicazioni presenti nella whitelist.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	In fase di implementazione attraverso l'applicativo Spiceworks al fine di rilevare presenza di software non autorizzato.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	L'elenco dei software autorizzati è in fase di completamento ed è costituito da un file excel gestito dal servizio Ced e salvato in una cartella ad accesso limitato su server.
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.	In fase di valutazione di un apposito software gestionale
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	L'infrastruttura virtuale esistente, offre questa possibilità all'occorrenza.

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.	Il servizio Ced definisce e mantiene la descrizione della configurazione sicura standard per ogni tipologia di sistema operativo. La descrizione è mantenuta all'intero di file word salvati in una cartella ad accesso limitato su server. Attività in fase di completamento.
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 sono attualmente gestite differenti tipologie di configurazione sicura standard per un singolo sistema operativo.
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.	Attualmente sono gestite le immagini di installazione per alcune postazione. Semestralmente, le configurazioni sicure standard vengo valutate per esser validate o eventualmente aggiornate in considerazione delle più recenti vulnerabilità e vettori di attacco.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Il servizio informatico definisce e mantiene la descrizione della configurazione standard di ogni tipologia di sistema. La descrizione è mantenuta all'intero di file word salvati in una cartella ad accesso limitato su server.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Per politica dell'ente eventuali sistemi compromessi vengono ripristinati utilizzando la configurazione standard.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Attualmente non è formalizzata alcuna procedura specifica di gestione dei cambiamenti.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione esistenti sono in corso di produzione e verranno a breve memorizzate off-line su hd esterno custodito in cassaforte protetta.

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 esistenti verranno memorizzate off-line su hd esterno custodito in cassaforte protetta. Le chiavi della cassaforte sono in possesso solo degli 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).	Per i collegamenti da remoto dall'esterno della si utilizzano le seguenti modalità: <ul style="list-style-type: none"> • logmein • team viewer Per il collegamento ai server dall'interno della rete viene utilizzato desktop remoto. Per i sistemi linux viene utilizzato secure shell
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Attualmente non vengono effettuate verifiche di integrità in modo sistematico, per l'esecuzione e il reperimento di applicazioni quando disponibile si predilige la verifica on line dell'impronta di integrità del singolo file
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.	Al momento non implementata
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.	Al momento non implementata
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Al momento non implementata
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Al momento non implementata
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Al momento non implementata

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.	L'ente sta valutando l'attivazione di un software per la gestione delle vulnerabilità (es. OpenVAS, GFI Languard) per poter effettuare l'esecuzione delle ricerche delle vulnerabilità ad ogni modifica significativa della configurazione.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Viene effettuata periodicamente (frequenza Bimestrale) una ricerca manuale delle vulnerabilità, sino alla futura attivazione di un software apposito.
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).	Al momento non implementata
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Al momento non implementata
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Al momento non implementata
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Al momento non implementata
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.	Una volta attivato un sistema per l'individuazione delle vulnerabilità, questo eseguirà le scansioni in modalità privilegiata utilizzando un account dedicato che non sarà utilizzato 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.	Attualmente gestito con IP statico e con utente con privilegi elevati dedicato
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	L'applicativo di gestione delle vulnerabilità che sarà attivato prevedrà un periodico aggiornamento delle più rilevanti vulnerabilità di sicurezza. Le scansioni manuali vengono effettuate con le versioni più aggiornate degli strumenti a disposizione.
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	Registrazione effettuata con il servizio alert del sistema antivirus in uso

4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'aggiornamento dei sistemi operativi è attivato sui client senza servizio centralizzato e per gli applicativi gestibili avviene periodicamente. Per gli altri applicativi sono in fase di creazione apposite Gruppo Policy di dominio
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Attualmente non sono presenti sistemi separati dalla 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.	Le impostazioni di scansione sono preventivamente definite e non sono modificabili dagli utenti.
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.	Le rilevazioni e le azioni correttive sono documentate tramite il sistema di ticketing e i report del sistema antivirus.
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.	Attualmente non implementata. Si prevede di attivare tale misura in futuro pianificando una verifica bimestrale
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.).	Il servizio Ced dovrà implementare un piano di gestione dei rischi con aggiornamento annuale in cui vengono valutati rischi e vulnerabilità, la loro gravità, il loro impatto ed a seguito dei risultati emersi dall'analisi del rischio, viene definito un apposito piano 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.	Le vulnerabilità saranno classificate secondo priorità e gestite secondo questo ordine. Il tutto verrà documentato all'interno di fogli di office automation
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.	Attualmente non implementata
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.	Attualmente non implementata

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 gli utenti con privilegi di amministratore hanno competenze adeguate e necessità operativa di modificare la configurazione dei sistemi. Gli utenti degli uffici non sono amministratori locali di macchina. Esiste su ogni macchina un utente amministratore di macchina utilizzato dal Ced
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Le utenze amministrative vengono utilizzate solo per effettuare operazioni che ne richiedano i privilegi. Il log degli accessi degli amministratori di sistema è in fase di attivazione. E' in fase di verifica la copertura dei sistemi di tale servizio per valutarne l'integrazione con ulteriori soluzioni. Mensilmente il servizio prevede la produzione di un report.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	E' in fase di implementazione l'analisi e la rimodulazione dei privilegi delle utenze amministrative per assegnare i soli privilegi necessari per svolgere le attività previste
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Attualmente non implementata
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'elenco degli utenti amministratori viene mantenuto dal servizio Ced. E' in fase di attivazione la procedura organizzativa per il mantenimento e la formalizzazione dell'autorizzazione.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Attualmente non gestito
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 configurazione ed assegnazione di nuovi client, l'utente local admin viene disabilitato, viene creato un nuovo user admin locale con password complessa conservata secondo criteri di sicurezza e mantenuta dal servizio Ced.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Attualmente non implementata

5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Attualmente non implementata
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Attualmente non implementata
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Attualmente non implementata
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.	Attualmente non implementata
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).	Sono in fase di configurazione le Group Policy di dominio che permettono di gestire l'autenticazione degli amministratori con password di elevata robustezza in ambiente Windows. Il servizio Ced definirà le politiche e le modalità opportuno ed implementabili anche per gli altri sistemi esistenti.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	In fase di implementazione per l'ambiente windows mediante policy di dominio
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	In fase di implementazione mediante Policy di dominio per quanto riguarda gli ambienti Windows. Per altri sistemi operativo è in fase di verifica la fattibilità e la modalità di implementazione
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	In fase di implementazione mediante Policy di dominio per quanto riguarda gli ambienti Windows. Per altri sistemi operativo è in fase di verifica la fattibilità e la modalità di implementazione
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	In fase di implementazione mediante Policy di dominio per quanto riguarda gli ambienti Windows. Per altri sistemi operativo è in fase di verifica la fattibilità e la modalità di implementazione
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	In fase di implementazione mediante Policy di dominio per quanto riguarda gli ambienti Windows. Per altri sistemi operativo è in fase di verifica la fattibilità e la modalità di implementazione
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.	Attualmente non implementata

5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	Attualmente non implementata.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Le utenze con privilegi amministrativi sono completamente separate dalle utenze senza privilegi amministrativi in possesso alla stessa persona ed hanno credenziali differenti.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze, in particolare quelle amministrative, sono nominative e riconducibili ad una sola persona. Tutte le utenze "anonime" sono in fase di revisione e saranno gestite secondo politiche che permetteranno di essere riconducibili ad 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 essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Tutte le utenze "anonime" sono in fase di revisione e saranno gestite secondo politiche che permetteranno di essere riconducibili ad una sola persona. Tali utenze saranno utilizzate solamente per situazioni di emergenza.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Attualmente gli accessi avvengono tramite Utente Amministratore di macchina, solo quanto non è possibile tramite utente Amministratore di dominio.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Da implementare
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Attualmente l'autenticazione non viene effettuata mediante 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.	E' attualmente installato presso l'ente il sistema antimalware Trend Micro Worry-Free Business Security che viene aggiornato in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	È in corso l'attività di attivazione previo verifica funzionamento dei software applicativi
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Attualmente non implementata
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.	La modifica della configurazione del sistema antivirus è bloccata mediante password in modo che gli utenti non possano alterare la configurazione effettuata dal servizio Ced.
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.	Mediante la console del sistema Trend Micro è possibile forzare manualmente l'aggiornamento dell'antimalware di ciascun dispositivo.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Attualmente non implementata
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Mediante apposita policy organizzativa dell'ente è definito che l'uso dei dispositivi esterni deve essere limitato per le attività aziendali
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Attualmente non implementata
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Attualmente non implementata
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Attualmente non implementata

8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Attualmente non implementata
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Attualmente non implementata
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Attualmente non implementata
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	In fase di implementazione mediante Policy di dominio
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	In fase di implementazione mediante Policy di dominio
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	In fase di implementazione mediante Policy di dominio
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	In fase di implementazione mediante Policy di dominio
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	In fase di implementazione mediante configurazione del sistema anti-malware
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 filtraggio del contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario è effettuato tramite il sistema attivo dal gestore delle caselle mail esterno all'ente
8	9	2	M	Filtrare il contenuto del traffico web.	Attivo sul 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).	Attivo sul sistema di posta esterno.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Attualmente non implementato
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Attualmente non implementato

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Viene effettuata una replica quotidiana con Veeam Backup delle principali Virtual Machine. La politica di backup è in fase di revisione per adeguarla alle misure di sicurezza richieste
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.	Le procedure di backup riguardano sia i sistemi operativi, che i dati che gli applicativi I sistemi sono molteplici e differenziati per supporto, periodicità e garantiscono un buon grado di storicizzazione nel tempo
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Vengono utilizzati i seguenti sistemi: <ul style="list-style-type: none"> • Backup Exec • Veeam Backup
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Vengono eseguiti ripristini periodici dei backpu.
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 sono conservati su nas custoditi in locali chiusi a chiave e ad accesso riservato agli addetti ced.
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.	Il nas viene acceso soltanto nella fascia orario adibita al backup. Stiamo inoltre acquistando un HDD esterno su cui posizionare le copie di backup e che sarà accessibile solo nel momento della copia.

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	L'ente effettua periodicamente un'analisi dei dati per valutare ed identificare quelli particolarmente rilevanti in tema di sicurezza, e per definire quali necessitano di crittazione.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Attualmente non implementata
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Attualmente non implementata
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	Attualmente non implementata
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Attualmente non implementata
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Attualmente non implementata
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.	Attualmente non implementata
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Attualmente non implementata
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Attualmente non implementata

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il firewall permette di gestire black-list.
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	Attualmente non implementata