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 Bolgare.xlsx è riportato in allegato al presente documento.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Su ogni dispositivo è installato un agente di controllo in grado di rilevare l'inventario di tutte le risorse.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	L'agente Logmein Pro installato su ogni dispositivo consente la rilevazione di anomalie e la generazione di allarmi (ticket) inviabili via mail e consultabili dalla console di controllo.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	L'agente Logmein rileva il traffico in ingresso e in uscita del dispositivo classificando in maniera automatica attraverso report i dispositivi più operosi.
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Il server DHCP attraverso l'inventario degli indirizzi hardware cataloga e monitora i log dei dispositivi connessi.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Tutti i dispositivi senza mac address registrato forniscono le informazioni dei dispositivi non ancora registrati e rilevati dalla rete.
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	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Soluzione da implementare tramite le funzionalità del sistema operativo del server.
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
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.	L'inventario generato in Central prevede di etichettare i dispositivi definendone stato, ubicazione e funzioni.
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.	Tramite software antivirus WithSecure vengono identificati e controllati dispositivi laptop, tablet, cellulari, pc a prescindere dalla loro appartenenza alla rete; qualora siano dispositivi esterni vengono tracciati attraverso la wifi o la rete cablata al loro primo

					accesso.
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.	Sistema non ancora implementato.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Vengono utilizzati i certificati dei sistemi operativi per l'accreditamento al dominio ed al gestore delle risorse di rete; in mancanza di questa autorizzazione non verranno resi disponibili dati o risorse condivise.

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. Installazione software sui client solo dagli amministratori.
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.	Il sistema antivirus installato in locale utilizza due componenti deep control e application manager per la gestione delle whitelist e delle blacklist dei software.
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).	Soluzione adottata ABSC 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.	Application manager (ABSC 2.2.1) esegue controlli periodici sulla lista dei software; solo l'amministratore può modificare tale lista.
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.
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,	L'agente locale Logmein rileva e genera l'inventario non solo dei sistemi operativi e di tutte le sue varianti, quali aggiornamenti e

				workstation e laptop.	patch, ma tiene traccia anche dell'installazione di qualsiasi software installato sul dispositivo.
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.	Misura ABSC 2.3.2
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.	Soluzioni non implementate non essendoci operazioni tali da crearne la necessità.

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	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.	Controllo periodico degli account attivi e controllo porte e patch tramite software di controllo in cloud per l'esecuzione massiva di comandi di patching
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.	I sistemi operativi non vengono distribuiti tramite immagine.
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	2	3	S	Le modifiche alla configurazione standard devono essere	Le modifiche standard vengono distribuite tramite cloud in modo

				effettuate secondo le procedure di gestione dei cambiamenti.	uniforme.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Immagini d'installazione memorizzate offline su NAS server.
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 sono a disposizione solo degli utenti amministratori.
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.
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.	Vengono utilizzati sistemi di integrità proprietari del sistema operativo e installate applicazioni solo con firma riconosciuta (UAC control).
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.	Alert registrato negli eventi di sistema.
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.	Piattaforma di ripristino del sistema operativo e in alcuni software funzionalità proprietaria dello stesso.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	La variazione di privilegi è gestita dal sistema di controllo di integrità dei dati del SO server.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Software non implementato.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Agenti di backup locale con ripristino alle impostazioni di configurazione standard o di fabbrica.

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'antivirus WithSecure scansiona e genera report sulle eventuali vulnerabilità sul sistema.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	L'Amministratore di Sistema utilizza la propria piattaforma cloud WithSecure Elements Vulnerability Management per controllare l'infrastruttura in automatico o con cadenza programmata, con esecuzione dei test di data breach.
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).	Funzione SCAP presente in WithSecure Elements Vulnerability Management.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Vengono eseguite join tra i vari report generati dal sistema WithSecure EVM-Central.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Antivirus scan di WithSecure registra le attività di scanning.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Sistema adottato per ABSC 4.2.2
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.	L'account dedicato alla piattaforma di gestione vulnerabilità WithSecure EVM non è utilizzato da nessun'altra attività di sistema ed è ad uso privilegiato dell'ADS.
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.	Funzionalità proprietaria di WithSecure EVM.
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.

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	Radar è un prodotto cloud interconnesso con una banca dati centralizzata aggiornata con le informazioni degli ultimi attacchi e delle nuove misure per far fronte ad essi.
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	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 attività di scansione vengono controllate e programmate dall'ADS secondo le 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 verificato che le vulnerabilità emerse dalle scansioni siano state risolte per mezzo di patch o manualmente.
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.	Vengono eseguiti 2 volte all'anno controlli per la gestione delle vulnerabilità esistenti introducendo eventuali misure risolutive con la rivalutazione del 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.).	È stata prevista la redazione del piano di gestione dei rischi, verrà compilato sulla scorta delle rilevazioni WithSecure EVM.
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 attribuita la priorità alle varie vulnerabilità.
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.	Vengono definite misure alternative al verificarsi di nuove vulnerabilità o di lunghi tempi di risoluzione delle stesse.
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.	I prodotti non standard o privi di firma digitale riconosciuta vengono testati in ambiente di test virtuale.

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.	E' attivato il log di sistema per registrare gli accessi come amministratore su PC, server, apparati di rete.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	In base alla funzione vengono attribuite le attività.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Funzione non implementata.
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	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Funzione non implementata.
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	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Viene tracciato nei log.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Funzione non implementata.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Funzione non implementata.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tutti i tentativi di log falliti vengono tracciati.
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	Vengono utilizzati sistemi di autenticazione a più fattori nei dispositivi mobili/fissi che lo prevedono.

				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).	Per le utenze amministrative vengono utilizzate credenziali complesse con simboli e caratteri alfanumerici.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Tutte le credenziali vengono valutate tramite software che ne valuta il grado di vulnerabilità.
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 password per tutti gli utenti.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Le password vengono gestite con cadenza semestrale.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Le password utilizzate non possono più essere riutilizzate prima di 12 mesi ed in alcuni casi per sempre.
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.	Funzionalità presente nei sistemi operativi ma per esigenze di software talvolta disabilitata.
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.	Misura non adottata.
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 essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Le utenze amministrative anonime sono utilizzate solo per emergenza e riconducibili a chi le ha utilizzate.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più	Tutte le reti sono provviste di dominio, non vengono usate utenze amministrative locali.

				elevato (e.g. dominio).	
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 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 contiene la gestione del firewall al suo interno.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	I syslog sono archiviati in locale e alcuni di essi in cloud.
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 piattaforma è in cloud, non alterabile.
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.	Il sistema WithSecure permette l'esecuzione degli aggiornamenti in maniera obbligatoria, rilevandone la corretta esecuzione o il suo fallimento.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	La piattaforma WithSecure risiede in cloud su server del produttore.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	E' stata data disposizione di limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	I servizi UTM monitorano l'accesso alla rete LAN e WAN.
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.	Le funzioni DEP e ASLR sono abilitate.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento	Gli agenti WithSecure e Logme installati vanno ad integrare gli

				delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	strumenti di contrasto proprietari dei 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.	Funzionalità integrata nei servizi UTM del firewall.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Funzionalità integrata nel sistema antivirus.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Funzionalità integrata nei servizi UTM.
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.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Funzionalità integrata nel firewall e nel servizio di antivirus.
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.	Funzionalità integrata nel servizio di antivirus.

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	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 policy di backup adottate prevedono il salvataggio in locale ed in cloud della VM server, dei dati e dei software in maniera completa ed incrementale.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Vengono utilizzati 2 sistemi di backup (Acronis backup per il cloud e Veeam backup per le macchine virtuali in loco).
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Vengono eseguiti periodicamente ripristini dei dati e verifica dei sistemi e dei dischi adibiti al 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	Viene effettuata l'analisi per i dati più rilevanti con distinzione di quali crittografare e quali no.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Non vengono utilizzati dispositivi portatili e attualmente non sono implementate policy di cifratura.
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.	Funzionalità integrata nei sistemi hardware e software del firewall.

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.	Funzione 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.	Funzione 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.	Funzione 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.	Funzionalità adottata sui server e sui sistemi di backup attraverso software proprietario del produttore
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Funzionalità adottata dal sistema firewall.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Funzionalità adottata dal sistema firewall.
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.
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.	Le copie dei file vengono effettuate mantenendo i privilegi iniziali.