Allegato:

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	La quasi totalità delle risorse attive (PC, portatili, stampanti, server, fotocopiatori) dispongono di un indirizzo IP per la loro identificazione all'interno della rete LAN comunale. L'inventario per le risorse attive sulla rete interna LAN viene eseguito per mezzo di un apposito software di rilevazione dispositivi di rete che ne rileva (a meno di anomalie) sia la parte hardware per i PC, sia la loro parte software con inclusa la rilevazione dell'indirizzo IP, del nome macchina e dell'utente collegato (sotto dominio windows). Ogni risorsa attiva (di rete e non di rete) è comunque individuata (da parte dell'ufficio predisposto a tale attività) da un numero di inventario dei beni strumentali dell'Ente.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Come descritto al punto 1.1.1 è in uso uno strumento automatico di inventariazione delle risorse attive connesse alla rete locale interna (LAN) comunale.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Il discovery dei dispositivi collegati alla rete con relativa segnalazione di anomalie (visibili all'interno dell'applicativo) è attuato per mezzo del medesimo software riportato ai punti 1.1.1. e 1.1.2.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	L'analisi del traffico lato web (per mezzo di apparato firewall che ne garantisce anche il filtro dei contenuti) per IP è mostrata su base di categorie definite per mezzo dello stesso sistema di filtraggio web.
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Il DHCP di rete è disattivato.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Server DHCP di rete non è presente.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'elenco di cui al punto 1.1.1 è in genere affidato al software di monitoraggio accessi interno alla rete LAN.

1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Per mezzo dello strumento automatico di cui ai punti precedenti ed inoltre come citato al punto 1.3.1, l'inventario software ed hardware per IP viene eseguito in genere con l'inserimento di nuovi apparati sulla rete interna comunale.
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.	Come meglio descritto nei punti precedenti, l'inventario delle risorse identificabili con indirizzo IP collegati alla rete comunale è gestito per mezzo di apposito software che esegue scansioni automatiche e ne memorizza IP ed altre caratteristiche collegate ove possibile.
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.	Di norma non sono ammessi dispositivi diversi da quelli censiti (di cui al punto 1.1.1). L'inventario è risultante dal software in adozione che riporta ove possibile diversi dettagli per ogni indirizzo IP rilevato. Nell'elenco di cui al punto 1.1.1 sono registrati, l'IP, il nome macchina, il nome utente dell'utilizzatore del PC in dominio (il personale è collegato amministrativamente ad un ufficio di riferimento) ed ove possibile anche il sistema operativo della macchina/PC. Possono sussistere casi eccezionali e provvisori di collegamento di macchine/PC diverse da quelle censite, come ad esempio da consulenti/aziende per le quali l'Ente ha un contratto di consulenza/supporto/manutenzione.
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.	Esistono dispositivi scollegati dalla rete comunale ed in uso dagli uffici (non collegati al software di inventario di rete) per i quali esiste inventario dei beni patrimoniali dell'Ente (es: smartphone per la Polizia Locale, Tablet per l'ufficio turismo, portatili per la biblioteca, smartphone per l'ufficio di protezione civile, etc).
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.	Misura al momento non implementata.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Misura al momento non implementata.

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.	E' disponibile un elenco di software utilizzabili da parte dell'Ente (es: software di compressione archivi, lettori di documenti pdf, browser di navigazione, applicazioni di uso ufficio quali LibreOffice, client di posta elettronica, etc) che comunque è in costante aggiornamento e rivisitazione. Inoltre, parallelamente a tale attività, tramite il software antivirus, già in uso dall'Ente, è possibile limitare automaticamente l'installazione e l'utilizzo di una serie di software classificabili in blacklist (detto elenco è in continua evoluzione/definizione/aggiornamento).
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.	L'implementazione della whitelist è derivata dal complemento rispetto alla blacklist (punto 2.1.1) funzione introdotta dal sistema antivirus.
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).	Vedere 2.2.1. Sono in uso sistemi di virtualizzazione.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Misura al momento non implementata.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'attività di rilevamento è eseguita non in modo non automatico per mezzo del software di inventario software ed hardware per IP in uso all'Ente che invece esegue scansioni automatiche dei dispositivi connessi alla rete (punto 1.3.1).
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.	Per quanto possibile si utilizzano software già in possesso dell'Ente per l'esecuzione di inventario software ed hardware per IP all'interno della rete comunale (LAN) dell'Ente.
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	Misura al momento non implementata.

				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.	Al fine di ridurre il livello di rischio, ove necessario sono valutate logiche di virtualizzazione con il fine di limitare/isolare verso la rete LAN possibili minacce ed al tempo stesso cercare di garantire il funzionamento di applicazioni necessarie per gli uffici (es: Pensioni S7 per l'ufficio personale, etc).

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.	Completata la fase di inizializzazione del sistema operativo (tipicamente "Windows"), le operazioni che di norma seguono sono (elenco non esaustivo): 1. collegamento in dominio windows del PC/Notebook in uso; 2. aggiungere le sole utenze di dominio relative all'ufficio a cui farà riferimento lo specifico PC/Notebook; 3. installazione del software necessario per le attività dell'ufficio (es: come da punto 2.1.1); 4. installazione dell'antivirus (con allineamento alla console centralizzata);
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.	Misura parzialmente implementata. Di norma la configurazione punta ad applicare gli aggiornamenti (di sicurezza e/o funzionalità) compatibilmente a possibili situazioni di blocchi/disservizi dovuti alla loro applicazione.
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.	Misura al momento non implementata.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati	Come riportato al punto 3.1.1.

				dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	In caso di compromissione di un sistema in esercizio ed in base alla gravità della problematica, dopo aver eseguito un'operazione di bonifica (rimozione virus con relativa scansione multipla anti-virus e correzione della falla informatica o guasto hardware), l'apparato viene ripristinato in base alla configurazione standard di cui al punto 3.1.1.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Non sono applicate modifiche che non siano contemplate da funzioni fornite dai sistemi in uso.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione delle macchine ritenute strategiche per l'Ente (es: sistemi operativi per apparati server, etc) sono memorizzate oltre che su unità NAS (collegate su rete LAN comunale) di norma anche su supporto esterno (HDD in off-line e/o su supporti DVD).
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 di cui al punto 3.3.1 sono poste in ambiente chiuso e ad accesso limitato (sala server).
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).	I firewall perimetrali sono impostati in modo tale da non avere regole in ingresso (es: esclusione di accesso diretto su protocollo RDP). L'eventuale amministrazione/gestione remota della rete comunale a delle PdL (Postazioni di Lavoro) organizzate solo per mezzo di canale VPN, oppure in alternativa per mezzo di software di controllo remoto che faccia uso di canali sicuri/crittografati.
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.	Misura al momento non implementata.
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.	Misura 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.	Misura al momento non implementata.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni	Misura al momento non implementata.

				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.	Misura 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.	Misura 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.	Il software usato per l'inventario hardware e software interno alla rete LAN comunale (di cui al punto 1.1.1) è in grado di eseguire scansioni interne per i PC collegati alla LAN comunale e fornire indicazioni utili su versione del software in uso al fine di poter procedere automaticamente dove possibile o manualmente all'applicazione degli aggiornamenti del sistema operativo e/o degli applicativi maggiormente utilizzati.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Del software di cui al punto 4.1.1, sono eseguiti controlli manuali quando possibile.
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).	Misura al momento non implementata.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Misura al momento non implementata.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Misura al momento non implementata.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Misura 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.	L'attività di verifica è svolta manualmente in base alla versione del software riscontrato e l'intervento di aggiornamento ha natura puntuale verso le singole macchine.
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.	Il software di cui al punto 4.1.1 è impiegato su una macchina (PC) utilizzata dal personale dell'ufficio informatica e le informazioni raccolte sono adoperate al fine del miglioramento delle condizioni/configurazioni interne alla rete comunale (LAN).
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il software di cui al punto 4.1.1 è aggiornato periodicamente secondo la licenza in uso. Il software non prevede aggiornamenti di verifica vulnerabilità di sicurezza.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Il software di inventario hardware e software in uso su rete LAN comunale, prevede attività di scansione che non possono essere profilate/configurate con servizi terzi. L'attività di informazioni sulle nuove minacce e vulnerabilità sono osservate di norma in fase di login alla console antivirus.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Ove possibile sono attivi in modo predefinito gli aggiornamenti automatici dei sistemi operativi e degli applicativi in uso per la parte client (PC di dominio). Per i sistemi operativi più strategici (es: Server) per i quali il possibile fermo operativo può compromettere la continuità operatività dell'Ente, l'aggiornamento delle patch è di norma attuato con metodi non automatici per limitare al minimo i possibili rischi introdotti da installazioni automatizzate. Tale azione è volta a minimizzare i casi in cui l'applicazione delle patch correttive possa in realtà introdurre gravi problemi legati al funzionamento degli stessi sistemi (uso di snapshots che altrimenti non esisterebbero in fase di aggiornamenti automatici). Per la parte Server sono attive configurazioni di replica (ed uso di snapshots in fase di applicazione manuale di aggiornamenti di sistema) delle macchine virtuali (macchine Windows Server in ambiente virtualizzato) al fine di offrire una ragionevole condizione di continuità del servizio anche a fronte di installazioni di patch che potrebbero bloccare/compromettere l'attività server dopo un

					aggiornamento. Per quanto riguarda l'installazione di patch non ancora automatizzate, si demanda tale azione ad una attività manuale in base ai software in uso.
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.	Per i sistemi (es: Notebook e PC) non collegati alla rete interna comunale di norma sono previste azioni di aggiornamento manuale delle patch di sicurezza. Gli aggiornamenti firmware delle stampanti/plotter/fotocopiatori sono applicati in seguito alla segnalazione di anomalie/malfunzionamento imputabili ad un problema firmware. Tale attività è erogata compatibilmente con il personale tecnico di cui l'Ente dispone.
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.	Misura al momento non implementata.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	In seguito all'adozione del software di cui al punto 4.1.1 sono di norma applicate le patch di sicurezza necessarie oppure in loro assenza/impossibilità di applicazione, saranno valutate possibili contromisure accettando un ragionevole rischio. Tale attività è erogata compatibilmente con il personale tecnico di cui l'Ente dispone.
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.	Misura al momento non implementata.
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.).	Rimane ancora da definire il piano di intervento per limitare/mitigare i possibili rischi. Tale attività sarà erogata compatibilmente con il personale tecnico di cui l'Ente dispone.
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.	Con il software di cui al punto 4.1.1 è possibile stabilire un'ordine di priorità della risoluzione delle vulnerabilità partendo da quelle più critiche (es: software obsoleto, sistema operativo giunto ad end-of-life, etc). Tale attività è erogata compatibilmente con il personale tecnico di cui l'Ente dispone.

					L’installazione delle patch per le vulnerabilità (di sicurezza) sono inoltre improntate sul: - possibile blocco dei sistemi imputabili all’applicazione delle patch stesse (da cui il punto 4.8.1); - mitigazione del rischio partendo dalle condizioni più critiche.
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.	In caso di assenza di patch utili alla risoluzione di una condizione critica di sicurezza nota, oppure in casi di dilatazione dei tempi di applicazione delle patch stessa saranno valutate contromisure alternative per la mitigazione del rischio dovuto alla vulnerabilità riscontrata. Tale condizione può trovare corrispondenza al punto 4.8.1.
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Misura al momento 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.	I privilegi amministrativi delle postazioni sono improntati sul buon funzionamento degli applicativi che richiedono tali diritti per il loro corretto funzionamento ed allo stesso tempo per l'esecuzione delle attività di aggiornamento per le stesse postazioni/PC. Per quanto riguarda l'unico tablet in uso all'ufficio turismo, l'accesso amministrativo è concesso all'unico soggetto (dipendente dell'ufficio turismo) che provvede, in autonomia, ad eseguire gli aggiornamenti di sicurezza (delle applicazioni installate e del sistema operativo).
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Le utenze amministrative (MS Server di dominio) definite al punto 5.1.1 sono registrate per sessioni di log-in e log-out così come le utenze di dominio.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Ogni utente di dominio è profilato in modo tale da poter accedere alla sola area di competenza (accesso al file-server attraverso le ACL di Microsoft per le sole cartelle/file del proprio settore/ufficio e per le applicazioni di back-office in uso al proprio settore/ufficio).

					Le utenze amministrative operano in ambito di manutenzione/gestione per il corretto funzionamento dei sistemi ma non in loro utilizzo ordinario.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Misura al momento non implementata. Le attività registrate per le utenze di dominio, a prescindere che siano di tipo amministrative (così come riportato al punto 5.1.2) comprendono l'azione di accesso (log-in e log-out) al dominio con inclusione dei tentativi falliti di log-in.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Rimane da adottare formale procedura di inventariazione delle utenze amministrative necessarie (es: per mezzo foglio di calcolo). Esistono utenze amministrative con finalità di servizio (es: funzionamento di software di back-office, per esecuzione di backup automatici, etc).
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Misura al momento 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.	Di norma ogni PC/Notebook che viene collegato al dominio viene impostato con almeno un profilo utente di dominio destinato al suo utilizzo (più di uno se riguarda una multi-utenza per lo stesso ufficio) ove possibile sono eseguite modifiche delle credenziali di accesso locale del dispositivo in modo da evitare potenziali accessi attraverso credenziali predefinite (di default) derivanti da utenze locali (es: evitare la presenza di account locali senza password).
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Misura al momento non implementata.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Misura al momento non implementata.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Misura al momento non implementata.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Misura al momento non completamente implementata (implementata solo in parte).
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	Misura al momento non completamente implementata (implementata solo in parte).

				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).	Le credenziali per le utenze in genere sono caratterizzate da complessità elevata mediante l'uso di numeri, lettere (maiuscole e minuscole) e di caratteri speciali. Le utenze amministrative che per diversi motivi non prevedono/possono utilizzare tale tipo di accorgimento (es: utenze di servizio), si cercheranno di adottare accorgimenti/contromisure per la riduzione dei possibili rischi.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Il dominio in uso obbliga le utenze ad impostare la propria password di accesso in base ad una certa complessità.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Sia le credenziali legate alle utenze amministrative (escludendo quelle di servizio, tipicamente quelle richieste ad esempio per il funzionamento di software di back-office dell'Ente), sia le utenze di dominio non amministrative sono impostate con scadenza/modifica ogni 180gg.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Nel caso di utenze amministrative di dominio, tale impostazione potrà essere adotta solo dopo il completamento del punto 5.2.1.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Misura al momento non implementata.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Misura al momento non implementata.
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.	L'accesso ai sistemi (server) avviene, di norma, tramite protocollo RDP per mezzo di utenze amministrative di dominio, ma per attuare tale tipo di accesso, l'utente è tenuto preventivamente ad autenticarsi a dominio come utente semplice. La logica adottata è quella di escludere accessi diretti.
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.	Le macchine che risultano avere un ruolo strategico per l'Ente sono i Server (di tipo virtualizzati) posti all'interno della rete comunale (LAN). Non sono previsti o presenti server in configurazione DMZ. Le uniche attività per le quali i Server sono impieganti è per l'erogazione di servizi su rete LAN (servizi di back-office ai diversi servizi/uffici dell'Ente quali ad esempio file-server ed sql-server con al loro interno la presenza di db per gli applicativi di back-office).
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono	Le utenze di dominio legate ai dipendenti (nelle more del punto 5.2.1) sono nominative non privilegiate e sono altresì distinte da

				corrispondere credenziali diverse.	quelle privilegiate degli amministratori di dominio con credenziali differenti.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Nelle more di quanto già definito al punto 5.2.1 e 5.10.1, anche se l'identificazione nominale (accesso nominale) dei soggetti utilizzatori rimane di tipo univoco.
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 in forma anonima rimangono circoscritte per le sole attività amministrative di mantenimento ed aggiornamento dei sistemi.
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).	Salvo casi in cui è necessario usare PC/Notebook non in dominio, l'operatività interna (su rete LAN) è di norma garantita per mezzo di utenze di dominio.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le singole credenziali amministrative (suddivise per servizio/tipologia) sono conservate in luogo non normalmente accessibile, chiuso e con chiave.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Per l'accesso ai sistemi informatici (server, apparati, PC) interni dell'Ente in smart-working si utilizzano sistemi VPN e/o di controllo remoto opportunamente configurati.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutti i PC/notebook/server (su base Windows e connessi alla rete LAN comunale) sono installati software antivirus con aggiornamento automatico. Nelle sedi remote per i PC connessi ad internet è comunque presente un antivirus con aggiornamento automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	I PC/notebook/server (su base Windows) presenti all'interno della rete possiedono una soluzione antivirus (di cui al punto 8.1.1) che introduce anche una parte firewall, che a secondo del tipo di configurazione adottata potrebbe non essere abilitata per problemi di gestione interna. Inoltre lo stesso antivirus in uso dall'Ente fornisce anche un componente “anti-exploit”. Si osserva che è sempre presente un firewall di tipo perimetrale sia per la rete comunale, sia

					per le sedi periferiche.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Misura al momento 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.	Misura al momento non implementata.
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.	L'antivirus è di tipo centralizzato ed è gestito per mezzo di una console web grazie alla quale è anche possibile forzare manualmente gli aggiornamenti delle definizioni antivirus.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Misura al momento non implementata.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'uso dei dispositivi non censiti di cui al punto 1.1.1 è strettamente limitato ai soli interventi necessari ed utili per l'Ente (es: attività di consulenza/supporto da parte delle aziende/software-house con l'Ente oppure riunioni/conferenze telematiche necessarie per l'attività amministrativa dell'Ente). Indicazioni operative sono contenute nell'Allegato B - "Disciplinare per un corretto utilizzo degli strumenti informatici, della rete informatica e telematica (internet e posta elettronica) e del sistema di telefonia fissa e mobile" presente nel Codice di Comportamento del Comune di Diano Marina.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Misura al momento 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.	Misura al momento 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.	Misura al momento 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.	I firewall perimetrali in uso presso l'Ente prevedono sistemi di filtraggio del traffico web che includono funzioni di rilevamento e blocco di codice malevolo dal web anche per mezzo di apposite liste con aggiornamento automatico dedicate allo scopo. L'uso di sistemi antivirus introduce un livello di protezione interno

					diversificato rispetto a quello del firewall perimetrale a beneficio delle risorse in rete.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Misura al momento non implementata.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	I firewall perimetrali di cui l'Ente dispone (di cui al punto 8.5.1) godono di liste aggiornate automaticamente grazie alle quali gli stessi firewall provano a limitare (per quanto tecnicamente possibile) il traffico generato verso i siti classificati come pericolosi/malware. Inoltre, i medesimi firewall sono dotati della funzione di geolocalizzazione delle richieste verso il web e sono in grado di bloccare le richieste per continente/nazione.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Per quanto possibile si tende a sconsigliare l'opzione di “autorun” dei dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Per quanto possibile si tende a sconsigliare l'esecuzione automatica dei contenuti dinamici.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	I client di posta, di norma, non prevedono l'apertura automatica dei messaggi di posta.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	I client di posta, di norma, non prevedono anteprime automatiche dei contenuti dei file, salvo che per le miniature delle immagini.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'antivirus è impostato in modo tale da eseguire una scansione automatica degli elementi/file avviati da unità esterne (supporti rimovibili).
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.	L'Ente dispone di un servizio di posta elettronica ordinaria (P.E.O.) in cloud dotato di sistemi di protezione antivirus ed antispam con la possibilità di impiego di liste (white-list e black-list) personalizzabili con blocco/filtri posti a monte delle stesse caselle di posta elettronica ordinaria. I sistemi di protezione di posta elettronica ordinaria prevedono un modulo sandbox come ulteriore strumento di protezione da link/url potenzialmente malevoli. Inoltre è prevista la personalizzazione ed il blocco di allegati già a livello di “mime file” (tipicamente eseguibili) anche se posti all'interno di file compressi, ovvero sono bloccati/disarmati file del tipo .exe, .bat, .msi, etc anche se posti dentro .zip, .rar, etc. già prima che gli stessi giungano nelle caselle di posta elettronica ordinaria dei destinatari.
8	9	2	M	Filtrare il contenuto del traffico web.	L'Ente dispone di firewall perimetrali in grado di filtrare

					automaticamente il traffico web in base a liste aggiornate automaticamente (con possibilità di generare nuove liste personalizzate) e filtrare il traffico web anche per localizzazione geografica delle risorse/richieste (vedere punto 8.6.1).
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).	Per il sistema di posta elettronica ordinaria e nel sistema di navigazione web (a livello antivirus) esistono impostazioni/regole utili a limitare lo scarico di specifici “mime file” (es: tipo .exe, .msi, .bat, .cab, etc.) o programmi al fine di incrementare il livello di sicurezza dell'infrastruttura (vedere punto 8.9.1 e 8.9.2). Inoltre è anche possibile impostare delle eccezioni mirate per sorgenti attendibili (es: DesktopTelematico dell'A.E., Software di aggiornamento legato a lettori pdf e simili, applicazioni di firma digitale per lo scarico degli aggiornamenti dei certificati legati all'uso della firma digitale, etc.).
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Misura al momento non implementata.
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.	Misura al momento non implementata.

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.	Ogni sera/notte viene eseguita una copia (su base differenziale) su NAS (in configurazione LUN di infrastruttura in alternanza con SMB/Share di rete) delle macchine virtuali dell’Ente sulle quali verte il funzionamento dell’Ente stesso. Inoltre è anche eseguita un’azione di replica delle macchine virtuali sul secondo server non di produzione. Il backup ha uno storico di 9 giorni. La copia prodotta off-line su HDD-USB esterno è effettuata in rotazione su due dischi removibili custoditi in cassaforti separate all’interno degli uffici dell'Ente con accesso controllato ed in luogo distinto dalla Sala Server.

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.	Come riportato al punto 10.1.1, le copie di backup riportano le immagini con logica differenziale delle macchine server utili al funzionamento informatico dell'Ente (nelle quali inoltre sono incluse la maggior parte dei dati/informazioni, applicazioni di back-office per gli uffici, nonché gli stessi Sistemi Operativi Server di produzione).
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Vedere punti punti 10.1.1 e 10.1.2. Si aggiunge la copia manuale di file/cartelle per mezzo di software di sincronizzazione tra sorgente (server) destinazione (NAS), riducendo i tempi di sincronizzazione rispetto al classico copia/incolla e fornendo uno strumento di recupero alternativo al software di backup.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Per aspetti legati a condizioni di licenza server e di spazio disco necessario, assunto che l'Ente non dispone di SAN o strutture equivalenti, non è possibile eseguire attività di ripristino di prova per le macchine virtuali di produzione, ma sono state eseguite con successo attività di recupero di file a campione al fine di verificarne preventivamente il corretto recupero puntuale in caso di necessità.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Le copie di sicurezza sono disponibili per mezzo di HDD-USB. I backup su cui sono presenti le immagini delle macchine virtuali dei server ottenute su base differenziale (comprensivi di buona parte dei dati ed applicazioni di back-office degli uffici) sono posti in luoghi chiusi e sotto chiave. I dischi HDD-USB su cui vengono eseguite le esportazioni dei dati di backup (di cui al punto 10.1.1, 10.1.2, 10.1.3) sono custoditi in cassaforti distinti e presenti presso l'Ente in uffici ad accesso controllato diversi dallla Sala Server.
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.	Come riportato al punto 10.1.1, 10.1.3 e 10.3.1 sono previste copie manuali di sicurezza da NAS (in cui sono presenti le immagini delle macchine virtuali comprensive di sistemi operativi, applicazioni e dati) verso dispositivi HDD-USB esterni utilizzati in rotazione per eseguire esportazioni/backup del repository in cui sono presenti i backup stessi. Gli HDD-USB sono collegati all'infrastruttura (on-line) per il solo tempo utile e necessario per eseguire materialmente le esportazioni/copie di backup (per il restante tempo sono

					fisicamente scollegati, ovvero off-line).

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	I dati di rilievo per l'Ente risiedono, di norma, all'interno dei server comunali (posti su rete locale LAN comunale). Esistono comunque procedure software in uso degli uffici (es: Demografci, Tributi, Contabilità/Ragioneria, etc) che sono fruibili direttamente da Web in logica SaaS presenti su Marketplace AgID. L'accesso ai dati (file/cartelle) è definito per mezzo di ACL (di Windows Server) per mezzo dei quale l'utente membro di un gruppo (ufficio/settore) può accedere al contenuto informativo (di quella particolare cartella/risorsa) in quanto dispone delle autorizzazioni corrispondenti al proprio ufficio/settore. Le fasi di crittografia, al momento (così come definito al punto 10.3.1) sono definiti solo per alcune fasi di backup (BAAS e NAS per backup dei soli dati collegati a cartelle e file dei server).
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Misura al momento 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.	I firewall perimetrali dell'Ente hanno sistemi di filtraggio dei contenuti per mezzo di liste (sia automatiche, sia personalizzate) che permettono il blocco (impostato di norma) su servizi di condivisione file (es: GDrive, DropBox, etc).
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.	Misura al momento 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.	Misura al momento non implementata.
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni	Misura al momento non implementata.

				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.	Misura al momento non implementata.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Misura al momento non implementata.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Misura al momento non implementata.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	I firewall perimetrali in uso sono dotati di sistemi web-filtering con black-list (automatiche e personalizzate) con inoltre la possibilità di eseguire un filtraggio in base alla geolocalizzazione delle risorse remote (è possibile bloccare/filtrare il traffico web anche per continente/nazione oltre che in base alle blacklist automatiche e personalizzate).
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.	Misura al momento non implementata.