Misure minime di sicurezza ICT per le pubbliche amministrazioni

Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

Il Sindaco
Realizzate in data 05/03/2020
Versione 1.0

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 dei dispositivi è redatto con software freeware denominato IP SCAN che fornisce informazioni minime circa l'indirizzo IP del dispositivo attivo in rete, l'indirizzo MAC ed il nome HOST. Il sistema di inventario delle risorse attive non è automatico.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Non si dispone di un software per l'aggiornamento automatico dell'inventario dei dispositivi quando nuovi dispositivi approvati vengono collegati in rete. A seguito di una nuova installazione hardware l'inventario è aggiornato in modo manuale con lo stesso software freeware IP SCAN. Prospettiva dell'Ente è di dotarsi di un sistema software di inventario automatico entro il 2020.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Per quanto concerne la gestione dell'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, non si dispone di un software di inventario automatico. L'inventario delle risorse di tutti i sistemi viene effettuato a cadenza mensile utilizzando il software freeware denominato IP SCAN che fornisce informazioni minime circa l'indirizzo IP del dispositivo attivo in

					rete, l'indirizzo MAC ed il nome HOST. Per quanto concerne l'elenco delle risorse di tutti i sistemi collegati alla rete si fa riferimento ad un elenco, prodotto manualmente, che riporta la configurazione standard di un Client e di un Server. Prospettiva dell'Ente è di dotarsi di un sistema software di inventario automatico entro il 2020.
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.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Non è presente un sistema software per per la produzione di un elenco di software autorizzati e relative versioni necessarie per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Al momento l'elenco dei software autorizzati è redatto manualmente considerando una macchina Client standard.

					Non è consentita l'installazione di software non compreso nell'elenco in quanto le macchine sono in dominio Active Directory (AD) ove i privilegi di installazione di software li detiene l'Amministratore di Sistema.
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.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Non è presente un sistema software automatico per eseguire scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. Tuttavia non è possibile per gli USERS (utenti standard) installare software non autorizzato in ragione dell'apparenza di tutte le macchine in dominio Active Directory (AD). I privilegi di installazione di nuovo software li detiene l'Amministratore di Sistema. Prospettiva dell'Ente è di dotarsi di un sistema software di scansione automatico entro il 2020.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato	

				nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Sono impiegate le seguenti configurazioni sicure standard per la protezione dei sistemi operativi. SISTEMI WINDOWS CLIENT - creazione di 2 partizioni sull'HD: una per i dati ed una dedicata al Sistema Operativo; - installazione del S.O. nella partizione C utilizzando la ISO ufficiale distribuita da Microsoft; - modifica nome account amministratore ed utilizzo di una password "robusta"; - join del Client al Dominio dell'Ente; - installazione automatica, tramite distribuzione da parte del dominio Active Directory, del sistema software Antivirus; - verifica abilitazione Firewall; - impostazione automatica degli aggiornamenti automatici di sicurezza e di sistema tramite il servizio di dominio WSUS (*Windows Server Update Services*); - eventuale installazione di software autorizzato (VEDI 2.1.1) SISTEMI WINDOWS SERVER - creazione di 2 HD separati: uno per i dati ed uno dedicato al Sistema Operativo;

					- installazione del S.O. nella partizione C utilizzando la ISO ufficiale distribuita da Microsoft in configurazione MINIMALE; - modifica nome account amministratore ed utilizzo di una password “robusta”; - join del Client al Dominio dell’Ente; - installazione automatica, tramite distribuzione da parte del dominio Active Directory, del sistema software Antivirus; - verifica abilitazione Firewall; - impostazione automatica degli aggiornamenti automatici di sicurezza e di sistema tramite il servizio di dominio WSUS (*Windows Server Update Services*); - eventuale installazione di software autorizzato (VEDI 2.1.1)
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.	
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.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Esiste una configurazione standard per workstation e server. Tali configurazioni sono implementate in base a quanto previsto al punto 3.1.1.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Esiste una scheda standard di configurazione HW e SW così come indicato al punto 3.2.1. Sistemi CLIENT in esercizio eventualmente compromessi sono ripristinati utilizzando un’immagine ISO del sistema operativo rilasciata direttamente da Microsoft; la configurazione SW

					standard è distribuita attraverso le GPO (Group Policy Object) di Active Directory (AD). Sistemi SERVER in esercizio eventualmente compromessi sono ripristinati utilizzando un Template standard ISO del sistema operativo rilasciata direttamente da Microsoft; Per i SERVER vengono create delle *snapshot* periodiche create con il software *Veeam Backup e Replication* che possono essere impiegate per il ripristino attraverso operazioni di *revert*.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Per i sistemi CLIENT le immagini sono memorizzate offline su chiavetta USB portabile, oppure vengono scaricate aggiornate al momento del bisogno dal sito internet del produttore (Microsoft). Per i SERVER le immagini di installazione sono memorizzate offline su un dispositivo NAS di rete oppure vengono scaricate aggiornate al momento del bisogno dal sito internet del produttore (Microsoft).
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature sono eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri tipo SSL, ovvero su canali sicuri)
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.	
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.	
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.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Nessuno degli utenti base, sulla base delle policy di dominio, è abilitato alla installazione/rimozione di software. Solo l'amministratore di sistema possiede i privilegi di installazione/rimozione di software specifico di terze parti.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	

4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	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.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Come strumento per la scansione delle vulnerabilità, sia su sistemi CLIENT sia su sistemi SERVER, viene impiegato il software antivirus AVAST BUSINESS che grazie ad una consolle centrale di amministrazione consente di avere la situazione aggiornata in tempo reale.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Le patch e gli aggiornamenti del software per il sistema operativo sono distribuite automaticamente a tutti i sistemi CLIENT e SERVER attraverso la funzionalità WSUS “Windows Server Update Services”. Le patch classificate da Microsoft come “critiche” sono automaticamente approvate e rese disponibili per l’installazione non appena i sistemi sono visibili “on line”.
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.	Tutti i dispositivi presenti nell’ente sono connessi a rete LAN cablata, non esistono dispositivi separati non connessi. La rete Wi-Fi presente all’interno dell’Ente è fisicamente separata dalla rete LAN comunale.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore	

				siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Le vulnerabilità emerse dalle scansioni sono ordinariamente risolte per mezzo di patch rilasciate dalla software-house (Microsoft). Non si è verificato il caso di adottare contromisure non standard.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Predisporre un documento in cui elencare quali apparati sono esposti a maggior rischio rispetto ad altri (es. per tipologia di servizio o per i tipi di dati trattati, etc) indicando precisamente il livello di rischio corrispondente (Alto, Medio e Basso). Per rischio si intende il tipo di criticità, che al verificarsi dell'evento malevolo, potrebbe influire gravemente sul funzionamento della struttura o di una sua parte.
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.	Sia i SO (Windows)server sia i So (10) cliente sono dotati di autonome funzioni di patching con il servizio automatico di Windows update (WSUS); le medesime funzioni si utilizzano per il software di produttività (Office).
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	A tutti gli utenti di dominio sono attribuite le Policy di "USERS". Nessun utente di dominio standard possiede i privilegi di amministratore. Le utente di amministrazione attive sono in capo al Servizio Sistemi Informativi.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Non sono attualmente registrati gli accessi amministrativi ai Server aziendali. L'Ente si fornirà di uno strumento che registri gli accessi degli utenze amministrative.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Le utenze amministrative sono in capo al Servizio Sistemi Informativi. Predisporre un atto di nomina per Amministratore di Sistema.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Ad ogni dispositivo collegato alla rete vengono sostituite le credenziali di default.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli	

				accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Non è implementato un sistema di autenticazione a due fattori. Per le utenze amministrative le credenziali rispettano i criteri di elevata robustezza (Passwording complesso).
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le credenziali delle utenze amministrative sono sostituite periodicamente.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le credenziali già utilizzate non possono mai essere riutilizzate (ultime 3).
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
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.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	È Assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali corrispondono credenziali diverse. A tutte le utenze è sempre abbinata un’anagrafica utente.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze amministrative sono nominative e sono 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.	Le utenze amministrative anonime "Administrator" di Windows, sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Una coppia di credenziali di accesso (Username, Password) sono custodite in busta chiusa in cassaforte. La busta reca il sigillo (firma) del segretario generale.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Per l'autenticazione su sistemi di gestione connessi alla LAN non si utilizzano 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.	Tutte le postazioni Client e Server connessi alla rete LAN sono dotati di sistema software di protezione Antivirus AVAST BUSINESS con consolle di gestione centralizzata per rilevare lo stato di aggiornamento della versione software e degli archivi di definizione dei virus. Alcuni Server sono dotati anche di software per la protezione da *Ransomware*, si tratta di CYBEREASON.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Esiste un dispositivo Firewall centralizzato nell'ambito del *Sistema Pubblico di Connettività* - contratto Quadro "RUPAR PUGLIA SPC" - per la fornitura del servizio di trasporto e sicurezza perimetrale.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	

8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	I dispositivi esterni utilizzabili sono generalmente PEN DRIVE USB il cui uso è impossibile da inibire in ragione dell'utilizzo dei token per la firma digitale. L'autorun è in ogni caso disattivato come policy di dominio. L'utilizzo di dispositivi di memoria esterna da parte del personale dipendente è limitato dall'utilizzo di cartelle condivise che consentono la condivisione di risorse in modo agevole e comunque sempre sotto il controllo continuo del software antivirus.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	I dispositivi esterni utilizzabili sono generalmente PEN DRIVE USB il cui uso è impossibile da inibire in ragione dell'utilizzo dei token per la firma digitale. L'autorun è in ogni caso disattivato come policy di dominio.

8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Le Macro degli elaboratori di testo (Word) sono disattivate per impostazione predefinita. L'utente ha la possibilità di attivarle in caso di necessità.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il client di posta predefinito è Microsoft Outlook. L'apertura automatica dei messaggi è disattivata per impostazione predefinita. L'utente ha la possibilità di modificare le impostazioni.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	L'apertura automatica dei contenuti dei file è disattivata per impostazione predefinita. L'utente ha la possibilità di modificare le impostazioni.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Da rendere obbligatoria la scansione della chiavetta. Al momento non è così.
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.	Esiste un antivirus/antispam centralizzato a livello server fornito dal Provider del servizio di posta elettronica. E' attivo anche un antivirus a livello client.
8	9	2	M	Filtrare il contenuto del traffico web.	Il traffico web è filtrato dal Firewall RUPAR PUGLIA SPC.
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).	La posta elettronica e tutto il traffico web è sottoposto al sistema di protezione perimetrale (Firewall del sistema RUPAR SPC) ed al software di protezione Antivirus AVAST BUSINESS. Al momento non sono previsti particolari blocchi su file non strettamente necessari per l'organizzazione e potenzialmente pericolosi (e.g. file .cab) Intenzione dell'Ente è di definire, di comune accordo con il Provider del servizio di posta elettronica ed Internet, il blocco di particolari file non strettamente necessari per l'organizzazione e potenzialmente pericolosi (e.g. file .cab).
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Una volta a settimana viene effettuata una copia completa (*Full*) dei Backup dei dati che coinvolgono tutti i server di produzione. Si tratta di *Snapshot* prodotte con il sistema software *Veeam Backup e Replication*. Durante i giorni della settimana invece sono programmate della snapshot periodiche di tipo incrementale.
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.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
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 backup sono effettuate su tre livelli di memorizzazione distinti e separati. Due livelli di copie sono mantenute su dispositivi NAS, separati dai dati di produzione, allocati fisicamente presso la sala CED del Comune; una copia invece viene delocalizzata su sistemi esterni all'Ente (in Cloud). La sala CED è dotata di misure di sicurezza antiintrusione come impianto di allarme, video sorveglianza, registrazione delle immagini per 3 giorni e porta blindata. Al momento le copie di backup non sono sottoposte a processi di cifratura.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Le copie di backup sono effettuate su tre livelli di memorizzazione distinti e separati. Un copia di backup dei dati viene delocalizzata su sistemi esterni con Provider Maggioli S.p.A..

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.	Occorre predisporre un documento, anche in sinergia con il DPO, di l'analisi per individuare la possibilità di aumentare i requisiti di riservatezza dell'Ente. Il reparto IT sarà a disposizione per le opportune valutazioni.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che	

				usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso URL presenti in una blacklist.	Il traffico è regolato da un sistema di protezione Firewall con Blacklist a livello centrale nell'ambito del contratto Quadro "RUPAR PUGLIA SPC" per la fornitura del servizio di trasporto e sicurezza perimetrale.
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.	