Comune di Porto Viro - Elenco delle misure minime implementate dall'ente

Elenco Misure Minime Agid

ABSC:1 CSC: 1 - INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Installato il servizio di Audit, del portale X-Infrastruttura, per la raccolta di informazioni destinate all'inventario. Tramite la funzione "INVENTARIO->Dispositivi" del portale "X-Infrastruttura", vengono visualizzati i dispositivi rilevati con i dati minimi necessari.	M
1.1.2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Come al punto 1.1.1 è stato implementato installato ed è attivo un servizio di Audit automatico che rileva tutte le macchine ed i softwere installati sui dispositivi.	S
1.1.3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
1.1.4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
1.2.2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	I dispositivi vengono rilevati automaticamente e gestiti manualmente.	M
1.3.2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	I dispositivi vengono rilevati automaticamente e censiti dal responsabile del servizio manualmente.	S
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	E' operativa la procedura di aggiornamento in modalità manuale dell'elenco delle risorse hw attive collegate alla rete. Per ogni dispositivo è indicato l'indirizzo IP. I dispositivi e gli IP sono rilevati con soluzione al punto 1.1.1	M
1.4.2	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.	E' operativa la procedura di aggiornamento in modalità manuale dell'elenco delle risorse hw attive collegate alla rete. Per ogni dispositivo oltre all'indirizzo IP è riportato quanto richiesto dalle misure.	S
1.4.3	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.	E' operativa la procedura di aggiornamento in modalità manuale dell'elenco dei dispositivi. Tali dispositivi non sono collegati alla rete.	A
1.5.1	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.		A
1.6.1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.		A

ABSC:2 CSC: 2 - INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
2.1.1	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'istallazione di software non compreso nell'elenco.	E' stato stilato l'elenco di software autorizzati con le relative versioni. L'agente di monitoraggio contiene la lista dei software installati.	M
2.2.1	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.		S
2.2.2	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).		S
2.2.3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.		A
2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	E' stato stilato l'elenco di software autorizzati con le relative versioni. L'agente di monitoraggio contiene la lista dei software installati suddivisi i 4 categorie "White llist", "Gray llist", "Black llist", "Non Gestiti". Dal nome delle stesse categorie, si individua quali sono i software "buoni" e quelli no, si lascia libera scelta all'ente nella gestione della quarta lista indicando in quale categoria dovranno finire quesi software non gestiti.	M
2.3.2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	L'inventario è mantenuto aggiornato mediante software che fa la scansione giornaliera	S
2.3.3	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.	Come per i punti 1.1.1 e 1.1.2 il servizio di Audit automatico rileva tutti i software installati la versione, ed eventualmente gli aggiornamenti cn relativa versione. In aggiunta la soluzione ATERA permette di verificare e aggiornare dove possibile le patch necessarie e automaticamente.	A
2.4.1	Utilizzare macchine virtuali e/o sistemi air-gapped1 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.		A

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

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vul-nerabilità di servizi e configurazioni.

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Gli amministratori di sistema provvederanno ad utilizzare solo configurazioni standard sicure (hardened) così come definite dagli standard di settore;	M
3.1.2	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.	La configurazione dei Sistemi operativi avviene secondo standard sicuri su tutti i pc viene installato antivirus e abilitati aggiornamenti del sistema operativo. Il personal firewall è attivato, abilitando in ingresso solamente ciò che viene richiesto dai vari software/servizi installati. Gli account non utilizzati vengono disabilitati, disattivati o eliminati i servizi non necessari, sono attivate patch di aggiornamento programmi e le porte sono chiuse se non utilizzate	S
3.1.3	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.		A
3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Gli amministratori di sistema provvedono ad utilizzare solo configurazioni standard sicure (hardened) così come definite dagli standard di settore; L'amministratore sta provvedendo a implementare un documento con le istruzioni per la configurazione di dispositivi standard.	M
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	in caso di necessità di ripristiono, verranno utilizzate le configurazioni standard. I dati sono principlamente in Cloud e/o salvati su server quindi una macchina compromessa viene ripristinata con le configurazioni standard in quanto non contenente informazioni o dati ma solo programmi.	M
3.2.3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.		S
3.3.1	Le immagini d?installazione devono essere memorizzate offline.	Le immagini sia dei server che delle postazioni di lavoro vengono memorizzate su posizioni offline; I software sono su supporti removibili e disponibili solo all'amministratore si sistema	M
3.3.2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Le immagini sia dei server che delle postazioni di lavoro vengono memorizzate su posizioni offline non accessibili ad utenti non autorizzati;	S
3.4.1	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).	Le operazioni di amministrazione remota di dispositivi avvengono: - RDP su VPN - RDP con connessioni securizzate - Atera chiave pubblica/privata RSA e codifica di sessione AES (256 bit). L?accesso al sistema avviene con 2FA - protocolli ssh	M

Comune di Porto Viro - Elenco delle misure minime implementate dall'ente

Elenco Misure Minime Agid

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
3.5.1	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.	questa attività viene eseguita dall'antivirus EPDR	S
3.5.2	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.	Gli allert vengono raccolti in maniera centralizzata dalla console cloud collegata all'antivirus EPDR installate in tutte le postazioni client e server	A
3.5.3	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.		A
3.5.4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.		A
3.6.1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.		A
3.7.1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.		A

ABSC:4 CSC: 4 - VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
4.1.1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	L'Ente ha implementato una funzionalità di acquisizione delle vulnerabilità tramite una sonda specifica che verifica e rendiconta tramite report semestrale le potenziali vulnerabilità del sistema ITC dell'Ente. In caso di programmazione delle attività ed in caso di modifiche significative delle configurazioni o delle infrastrutture	M
4.1.2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Vedi punto precedente 4.1.1	S
4.1.3	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).		A
4.2.1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.		S
4.2.2	Verificare che i log registrino le attività deis istemi di scanning delle vulnerabilità.		S
4.2.3	Verificare nei log da presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.		S
4.3.1	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.	vengono eseguite scansioni di vulnerabilità in modalità privilegiata, sia localmente e sia da remoto, utilizzando un account dedicato che non viene usato per nessun'altra attività di amministrazione.	S
4.3.2	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.	E' vincolata 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.	S
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il sistema di verifica e controllo delle vulnerabilità e affidato a una azienda esterna regolarmente contrattualizzata che garantisce l'aggiornamento del prodotto e la sicurezza dell'infrastruttura ITC	M
4.4.2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	vedi punto 4.1.1	S
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'Ente ha implementato un sistema di aggiornamento automatico gestito dalla piattaforma denominata Atera con cui vengono gestiti gli aggiornamenti del Sistema Operativo e sia per le applicazioni.	M

Comune di Porto Viro - Elenco delle misure minime implementate dall'ente

Elenco Misure Minime Agid

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	L'Ente non dispone di macchine al di fuori della rete, vengono aggiornate tutte automaticamente dalla rete mentre i telefoni mobili e tablet vengono aggiornati di volta in volta che si presentano gli aggiornamenti. Periodicamente il personale del CED provvede a manutenere questi dispositivi manualmente.	M
4.6.1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Le policy implementate vengono mantenute costantemente per tutti i cicli di scansione	S
4.7.1	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.	Periodicamente verrà valutata la scansione delle vulnerabilità e saranno prese le opportune azioni previste per la risoluzione dei problemi rilevati. In pratica vengono pianificate e implementate le remediation	M
4.7.2	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.		S
4.8.1	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.).	VIn sede di attività di scansione delle vulnerabilità viene sempre redatto un verbale dove viene riportata un?analisi del rischio	M
4.8.2	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.	Lo strumento per le scansioni attribuisce in maniera automatica livelli di priorità alle vulnerabilità rilevate che vengono poi valutate per l?implementazione	M
4.9.1	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.		S
4.10.1	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.		S

ABSC:5 CSC: 5 - USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
5.1.1	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 amministrazione sono limitati al personale adeguatamente formato. Per gli accessi esterni, le aziende incaricate vengono adeguatamente istruite e responsabilizzate non che l'accesso monitorato tramite firewalle x-log in cloud.	M
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	E' installato apposito agente che registra gli accessi attraverso la generazione di log sicuri e non modificabili. L'amministratore di sistema adotta quanto previsto da questa misura;	M
5.1.3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.		S
5.1.4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Le attivitò di autenticazione e operatività delle utenze amministrative sono raccolte nei log dei server che si occupano dell'autenticazione e nello strimento x-log.	A
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Verrà adottato un Regolamento nel quale sarà previsto l'individuazione di una lista delle utenze amministrative, la relativa custodia e le necessarie autorizzazioni	M
5.2.2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	L'inventario degli amministratori di sistema viene individuato con lo strumento X.LOG per quanto relativo ai server dell'ente. In sede di definizione l'elenco con le appropriate nomine all'interno del GDPR.	A
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	L'amministratore di sistema adotta quanto previsto da questa misura; Implementata ulteriore verifica per alcune apparecchiature a noleggio e gestite esclusivamente dalla ditta fornitrice (fotocopiatori)	M
5.4.2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.		S
5.4.3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.		S
5.5.1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Le attivitò di autenticazione delle utenze amministrative sono raccolte nei log dei server che si occupano dell'autenticazione e nello strimento x-log.	S
5.6.1	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.		A
5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	L'amministratore di sistema adotta quanto previsto da questa misura. Verrà comunque implementata e forzata la complessità delle credenziali tramite policy di sistema	M
5.7.2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Implementato studio di fattibilità per l'implementazione di password adeguatamente sicure.	S

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Gli amministratori di sistema sono soggetti ad una policy di cambio password (complessa) che si attiva ogni 60 giorni.	M
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Gli amministratori di sistema sono soggetti ad una policy di cambio password (complessa) che impedisce il riutilizzo delle password mantenendo uno storico degli hashcore di 1 anno.	M
5.7.5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Gli amministratori di sistema sono soggetti ad una policy di cambio password (complessa) che impedisce il cambio password per almeno 24 ore dal precedente.	S
5.7.6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Gli amministratori di sistema sono soggetti ad una policy di cambio password (complessa) che impedisce il riutilizzo delle password mantenendo uno storico degli hashcore di 1 anno.	S
5.8.1	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.		S
5.9.1	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.		S
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Sono state impostate utenze e credenziali diverse per attività di lavoro e attività di amministrazione del sistema. Ogni utente che deve disporre di privilegi amministrativi possiede due utente: una senza tali privilegi e una con tali privilegi.	M
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le password di amministrazione sono create per individuare l'utente autorizzato o la ditta esterna autorizzata alle attività di amministrazione, in quanto le credenziali sono nominative.	M
5.10.3	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 credenziali di amministrazione sono utilizzate esclusivamente per attività di emergenza. Vengono usate esclusivamente utenze amministrative nominali.	M
5.10.4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Prima dell'inserimento in dominio dei dispositivi viene creata un utenza amministrativa locale gestita secondo gli standard di configurazione. A seguito dell'inserimento in dominio, l'utenza viene disattivata.	S
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Ciascun utente con privilegi amministrativi nominale segue gli standard di conservazione definiti dal Comune. Le aziende terze consevano le credenziali in modo da preservarne la disponibilità e riservatezza.	M
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Gli addetti sono stati adeguatamente edotti sulla corretta gestione delle credenziali amministrative	M

ABSC:8 CSC: 8 - DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
8.1.1	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 windows è stato installato uno strumento di ?Endpoint Security? per la protezione totale delle postazioni. Gli strumenti sono configurati per aggiornamento automatico.	M
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.	E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura; E' implementato un firewall perimetrale che interagisce con il cliente locali installati sulle singole postazioni. Personal Firewall e IPS implementati tramite il prodotto di Endpoint protection	M
8.1.3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Sui sistemi in cui è installata la suite di ?Endpoint Security? è prevista la gestione centralizzata degli eventi	S
8.2.1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	E' installato sui dispositivi un software/agente di sicurezza "Endpoint Security" che è dotato di apposita funzionalità per poter soddisfare a questa misura;	S
8.2.2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi antimalware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	E' installato sui dispositivi un software/agente di sicurezza "Endpoint Security" che è dotato di apposita funzionalità per poter soddisfare a questa misura;	S
8.2.3	L'analisi dei potenziali malware è effettuata su di un?infrastruttura dedicata, eventualmente basata sul cloud.	E' installato sui dispositivi un software/agente di sicurezza "Endpoint Security" che è dotato di apposita funzionalità per poter soddisfare a questa misura;	A
8.3.1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è concesso l?uso di strumenti che non siano di proprietà dell?Ente, specificato anche in apposito regolamento.	M
8.4.1	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.	Tale funzionalità sono attive tramite strumenti integrati nei sistemi operativi e tramite il rilevamento e confinamento delle vulnerabilità dello strumento EPDR installato in tutti i dispositivi dell'ente.	S
8.4.2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Gli strumenti aggiuntivi forniti dal produttore dei sistemi operativi sono stati installati. In aggiunta è utilizzato il software EPDR in tutti i dispositivi.	A
8.5.1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.		S
8.5.2	Installare sistemi di analisi avanzata del software sospetto.	Il software di EPDR installato in tutti i dispositivi dell'ente analizza i software in esecuzione. L'analisi viene effettuata tramite protezione basata su firme e tramite analisi delle operazioni realtime.	A

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
8.6.1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Nel firewall della rete è attivo un servizio di Web Proxy e Web Filtering che impedisce la visita di siti considerati sospetti, malevoli o di cattiva reputazione.	S
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' installato sui dispositivi un software/agente di sicurezza "Endpoint Security" che è dotato di apposita funzionalità per poter soddisfare a questa misura;	M
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Implementata mediante GPO del dominio.	M
8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il servizio di posta elettronica è gestito e ospitato su servizi cloud.	M
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file.	Implementata mediante GPO del dominio.	M
8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	E' installato sui dispositivi un software/agente di sicurezza "Endpoint Security" che è dotato di apposita funzionalità per poter soddisfare a questa misura;;	M
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	La posta elettronica viene gestita e ospitata su servizi cloud che effettuano controlli antispam e antivirus prima di recapitare la posta (in uscita e in entrata). I controlli sono effettuati sulla base di score calcolati realtime e sulla base di database di segnalazione.	M
8.9.2	Filtrare il contenuto del traffico web.	E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura. E' presente inoltre un Firewall WatchGuard dotato di apposita funzione di content filtering.	M
8.9.3	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).	Il servizio cloud di posta elettronica blocca tutti gli allegati considerati malevoli, sulla base dell'estensione e del contenuto. E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura. E' presente inoltre un Firewall dotato di apposita funzione di content filtering.	M
8.10.1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	In automatico tramite Enpoint protection con funzione di EPDR	S
8.11.1	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.	In automatico tramite Enpoint protection con funzione di EPDR	S

ABSC:10 CSC: 10 - COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC_ID#	*Descrizione*	*Modalità di implementazione*	*Liv*
10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Per i server gestionali vengono seguite politiche di retention che consentono un ripristino della macchina con i dati degli ultimi due mesi con cadenza settimanale. In base all'importanza del servizio sono presenti politiche di retention aggiuntive su base giornaliera e mensile che estendono i punti di ripristino utilizzabili. I dati di lavoro delle postazioni client vengono salvati in un documentale centralizzato che è sottoposto alle politiche di cui sopra. Il sistema di disaster recovery è configurato per resistere ad attacchi di tipo ransomware.	M
10.1.2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Le procedure di backup coinvolgono il sistema operativo nella sua interezza (tramite virtualizzazione).	A
10.1.3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	I punti di ripristino vengono salvati in multiple posizione (offline). In caso di fallimento di uno dei sistemi, è disponibile il sistema secondario di DR.	A
10.2.1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Viene eseguita periodicamente per i dati del gestionale (su server) una prova di ripristino periodicamente.	S
10.3.1	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.	Viene eseguita la cifratura dei dati trasmessi in cloud. I dispositivi di memorizzazione in locale non sono accessibili ad utenti non autorizzati e vengono crittografati tramite funzionalità dei sistemi di DR e dei sistemi operativi.	M
10.4.1	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.	I sistemi di DR si trovano su sedi remote (dell'ente) rispetto ai sistemi primari. In questo modo eventi fisici avvenuti sull'uno non coinvolgono l'altro. Inoltre i sistemi DR sono configurati in modo da non avere vulnerabilità ad attacchi di tipo ransomware che minano alla disponibilità dei dati.	M

ABSC:13 CSC: 13 - PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l’esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l’integrità delle informazioni rilevanti

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
13.1.1	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	Eseguita mappatura dei dati dell'ente in sede di redazione de registro delle attività di trattamento tramite servizio GDPR dedicato.	M
13.2.1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti		S
13.3.1	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.		A
13.4.1	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.		A
13.5.1	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.		A
13.5.2	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.		A
13.6.1	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.		A
13.6.2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.		A
13.7.1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.		A
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist.	L'Ente ha implementato un sistema di firewall perimetrale con le funzionalità di backlist.	M
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist.	L'Ente ha implementato un sistema di firewall perimetrale con le funzionalità di backlist.	M
13.9.1	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.		A