AGenzia per l'Italia Digitale

ABSC_ID			Descrizione	Implementazione	Livello	Link/Allegati
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario è gestito tramite il software 'OCS Inventory', accessibile al seguente indirizzo 'http://intranet.tv.prov.local'. Questo sistema permette di avere a disposizione un catalogo completo delle macchine connesse, dei software installati, dei dati degli utenti collegati. L'inventario degli apparati di rete (switch) viene gestiti dal software HP ProCurve Manager (HPProCurveManager.prov.tv.local); quello delle stampanti di rete è acquisibile interrogando il server di stampa (ProvTVspool86.prov.tv.local). //IDENTIFICARE SOFTWARE MONITORAGGIO TELECAMERE E SISTEMA HONEYWELL	M	OCS Inventory

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
1	1	2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Questo punto è gestito tramite 'OCS Inventory', accessibile tramite il seguente indirizzo 'http://intranet.tv.prov.local'. Attraverso policy Windows, installiamo l'agent di 'OCS Inventory'. Questo software permette di avere a disposizione un elenco completo di molti aspetti che riguardano la rete della PA Provincia di Treviso (e.g. Traffico dati), le macchine connesse, i software presenti e altro. Si rende noto che questo punto viene inteso solo per le postazioni di lavoro riferibili agli utenti. L'elenco è automatizzato	S	OCS Inventory
1	2	1	Implementare il “logging” delle operazione del server DHCP	//QUESTO PUNTO AL MOMENTO NON VIENE GESTITO 10.100.200.157-158	S	
1	2	2	Utilizzare le informazioni ricavate dal “logging” DHCP per migliorare l’inventario delle risorse e identificare le risorse non ancora censite	//QUESTO PUNTO AL MOMENTO NON VIENE GESTITO	S	
1	3	1	Aggiornare l’inventario quando nuovi dispositivi approvati vengono collegati in rete	Questo punto è gestito tramite 'OCS Inventory'. Attraverso policy Windows, installiamo l'agent di tale programma e all'avvio successivo abbiamo l'elenco aggiornato con le ultime macchine che hanno effettuato l'accesso alla rete.	M	OCS Inventory

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
1	3	2	Aggiornare l’inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete	Questo punto è gestito tramite 'OCS Inventory', accessibile tramite il seguente indirizzo 'http://intranet.tv.prov.local'. Attraverso policy Windows, installiamo l'agent di 'OCS Inventory'. Questo software permette di avere a disposizione un elenco completo di molti aspetti che riguardano la rete della PA Provincia di Treviso (e.g. Traffico dati), le macchine connesse, i software presenti e altro. Si rende noto che questo punto viene inteso solo per le postazioni di lavoro riferibili agli utenti. L'elenco è automatizzato	S	OCS Inventory
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	Il catalogo dei dispositivi è contenuto nel file allegato "Schema_Reti2017"; quello delle stampanti di rete è acquisibile interrogando il server di stampa (ProvTVspool86.prov.tv.local). L'elenco completo dei server è contenuto nel file allegato "A_SchemaServer2017". ELENCO APPARATI DI VIDEOSORVEGLIANZA, SICUREZZA	M	Schema_Reti_2017.odt 2017-09-26 08:41:19 A_SchemaServer2017.ods 2017-09-26 08:41:57

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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	Questo punto viene gestito tramite 'OCS Inventory'. L'ufficio 'Manutenzione e Gestione Hardware e Software' dell'ufficio CED della PA Provincia di Treviso. Tramite incrocio di dati tra 'OCS Inventory' e l' 'Active Directory' permette di sapere l'ufficio associato all'utente. L'incrocio dei dati del software 'OCS Inventory' e del server DHCP permette il riconoscimento di unità personali dal momento che non hanno l'agent OCS installato	S	OCS Inventory
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.	L'elenco dei software autorizzati è mantenuto negli allegati "Software Client" (DA COMPLETARE) e "Software Server".	M	SoftwareClient.ods 2017-10-06 10:14:46 SoftwareServer.ods 2017-10-06 10:17:54

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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.	Questo punto è gestito dall'ufficio 'Manutenzione e Gestione Hardware/Software' dell'ufficio CED della PA Provincia di Treviso. Per mezzo di policy Windows e di attività amministrative in Active Directory, è possibile l'installazione di programmi nelle macchine, cui l'uso è concesso alle utenze, che sono inseriti all'interno di una whitelist in cui sono presenti i software strettamente necessari per lo svolgimento delle attività lavorative dell'ente di cui sopra. Tutto ciò è valido salvo per gli amministratori di macchina, che possono installare applicativi aggiuntivi, e considerando che ad ogni rielaborazione del documento questi software verranno eliminati. La nostra whitelist è riferita al file in allegato.	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)	// QUESTO PUNTO AL MOMENTO NON VIENE GESTITO	S	
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato	Utilizzando lo strumento 'OCS Inventory', monitoriamo tutti i software presenti sul client: periodicamente (DECIDERE LA CADENZA) questo elenco viene confrontato con il catalogo dei software ammessi.	M	OCS Inventory

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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	//DEVE ESSERE IMPLEMENTATA UNA LISTA DI PROGRAMMI CHE VENGONO ESEGUITI ALL'INTERNO DEI SERVER NEL FILE in allegato. Questo punto è gestito tramite 'OCS Inventory'. Attraverso policy windows, installiamo l'agent di tale programma e al prossimo avvio abbiamo l'elenco aggiornato con le ultime macchine che hanno effettuato l'accesso alla rete della PA Provincia di Treviso. Per quanto concerne i server, è presente un elenco degli stessi reperebile nel file allegato	S	A_SchemaServer2017.ods 2017-09-26 11:12:18
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Vengono applicate le impostazioni di sicurezza fornite da Windows; vengono inoltre applicate puntualmente le policy di sicurezza definite a livello di dominio. Per ogni nuovo client agganciato alla rete vengono preventivamente utilizzate queste regole.	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	Verificare le policy da imporre (servizi attivi con win firewall, porte da chiudere, ecc.)	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
3	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall’organizzazione	Questa è definita tramite impostazioni di sicurezza fornite da Windows e dalle policy di Dominio. Per i server Linux vengono ristretti i servizi attivati al minimo indispensabile (http, https, se necessari ftp e servizi di posta).	M	
3	2	2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard	Vengono mantenute in archivio le immagini delle macchine virtuali standard e quelle delle macchine "critiche" per il sistema: da queste immagini è quindi possibile effettuare un ripristino secondo configurazioni standard.	M	
3	2	3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti	//DEFINIRE PROCEDURA PER LA MODIFICA DELLE CONFIGURAZIONE STANDARD	S	
3	3	1	Le immagini d’installazione devono essere memorizzate offline	Questo punto è gestito dal personale dell'ufficio 'Manutenzione e Gestione Software/Hardware'. Il procedimento standard che viene seguito prevede l'installazione del sistema operativo, la cui immagine viene salvata su dispositivi di archiviazione offline, l'accreditamento della stessa perchè possa accedere alla rete e l'installazione dei programmi riconosciuti per mezzo di policy Windows. //SPECIFICARE DOVE SONO MANTENUTE LE IMMAGINI	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
3	3	2	Le immagini d’installazione sono conservate in modalità protetta, garantendone l’integrità e la disponibilità solo agli utenti autorizzati	Questo punto è gestito dall'ufficio 'Manutenzione e Gestione Hardware/Software' dell'ufficio CED della PA Provincia di Treviso che si occupa di mantenere offline le copie delle immagini d'installazione (da prevedere modalità di salvataggio off-line per i server)	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)	Sui server Windows e sugli switch queste operazioni vengono eseguite soltanto dalla rete locale o tramite connessione VPN alla rete locale, quindi da una rete sicura. Sui server Linux vengono eseguite tramite connessione SSH. //VERIFICARE TELECAMERE	M	
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	Questo punto è gestito direttamente dal sistema operativo Windows, il quale impedisce che l'utente possa accedere alle cartelle di sistema in cui sono contenuti i file fondamentali per il corretto funzionamento dell'interno SO -Sistema Operativo-. All'interno dell'ambiente Windows, tuttavia, è presente la possibilità tramite 'cmd' -Command Prompt- di verificare lo stato di salute dei file di sistema e cercare eventuali vulnerabilità. Vi sono varie possibilità di scelta riguardanti i tipi di file di cui eseguire la scansione, in base alle necessità e ai problemi che coinvolgono la macchina. Un esempio di comando è 'scannow'. Oltre ovviamente all’utilizzo dell’antivirus.	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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.	//Vedere servizio su AGID che fa ciò"	M	
4	1	2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura	Questo punto al momento è gestito solo all'interno dei server web in cui è presente un plug-in Joomla 'Admin Exile'. Questo plug-in è sempre attivo. PROCEDURA Agid da ripetere periodicamente	S	
4	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità	//QUESTO PUNTO AL MOMENTO NON VIENE GESTITO. Da verificare procedura e modalità per ottenere i log di sistema	S	
4	2	2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	//QUESTO PUNTO AL MOMENTO NON VIENE GESTITO. Da verificare procedura e modalità per ottenere i log di sistema	S	
4	2	3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile	Questo punto al momento è gestito all'interno dei server web, ed in particolare in quelli in cui è presente il plug-in Joomla 'Admin Exile'. E' possibile avere un elenco degli attacchi di un singolo IP verso il target. E' stata studiata una procedura che mira a bloccare sul SonicWall - firewall presente nella sala server dell'ufficio CED della PA Provincia di Treviso- questo indirizzo IP. Si lasciano in allegato i file ALLEGATO N°x e ALLEGATO N°y riguardanti tali procedure	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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	Utilizzo del sofware Agid per questa funzione	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	Utilizzo del sofware Agid per questa funzione	S	
4	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza	VEDI PUNTO 4.1.1	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"	Questo punto è gestito tramite l'utilizzo di 'AVG Admin Console', componente server che monitora lo stato delle macchine e che permette l'accesso da remoto alle stesse qualora presentassero un problema. Il requisito perchè questo sistema funzioni è che ci sia AVG installato all'interno della macchina. AVG è un antivirus installato in tutte i computer interni alla rete della Provincia. Per il sistema di posta elettronica si fa riferimento al sofware ClamAV	S	
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni	L'aggiornamento dei sistemi e dei programmi avviene attraverso le policy di Windows e l'utilizzo del portale WSUS. Per tutti i software "non-windows" l'aggiornamento viene effettuato solo da utenti amministratori.	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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	All'interno del sistema sono presenti solo alcuni sistemi Air Gapped (monitoraggio traffico stradale, controllo pompe sottopassi, eliminacode centri per l'impiego, pc stamperia, pc posizioni INAIL presso ufficio personale): su questi sistemi normalmente non vengono applicati aggiornamenti poichè inficerebbero l'uso dei software lì installati.	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	Questo punto è gestito dal personale dell'ufficio 'Manutenzione e Gestione Software/Hardware' che si occupa di effettuare i dovuti controlli in maniera puntuale e periodica. Verrà stilato un documento in cui vengono segnalate eventuali anomalie	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	All'applicazione di patch o nuove regole di sicurezza viene eseguita una scansione così come richiesto al punto 4.1.1 .	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	Questo punto è gestito dal personale dell'ufficio 'Manutenzione e Gestione Software/Hardware' che si occupa di controllare periodicamente la presenza di nuovi update -aggiornamenti- che vadano a verificare la disponibilità di patch che colmino la vulnerabilità qualora la stessa rappresenti un più alto livello di rischio per il sistema di quanto non era stato valutato precedentemente	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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.)	Questo punto è gestito dal responsabile del Settore Sistemi Informatici della Provincia di Treviso. (Necessità di definire una scaletta/procedura di gestione)	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	Questo punto è gestito dal responsabile del Settore Sistemi Informatici della Provincia di Treviso. (Necessità di definire una scaletta/procedura di gestione)	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	Questo punto è gestito dal personale dell'ufficio 'Manutenzione e Gestione Software/Hardware' che si occupa di controllare periodicamente la presenza di nuove vulnerabilità all'interno del sistema della PA Provincia di Treviso, gestirne il rischio e valutare se lo stesso possa essere accettabile oppure no. Qualora non fosse accettabile, occorre provvedere alla ricerca di patch per colmare il gap di sicurezza presente. Se ciò non fosse possibile, effettuare una ricerca di software alternativo che possa sostituire in tutto e per tutto i servizi offerti dal precedente e che abbia un più alto grado di sicurezza o un basso indice di rischio per la vulnerabilità: la lista dei programmi utilizzati è contenuta nell'allegato n°x	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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	Questo punto è gestito per alcuni sistemi “mission critical” esistono ambienti di test paralleli a quelli di produzione (ad esempio ADS - applicativo per gli atti amministrativi-); per altri prodotti sviluppati internamente vengono creati ambienti temporanei per testare le modifiche dei sistemi	S	
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.	A livello di dominio è stato individuato un gruppo di amministratori formati e competenti per svolgere operazioni di amministrazione, per altro rientrante nelle loro normali funzioni operative. In alcuni casi, l'utilizzo di particolari software richiede che l'utente sia amministratore del client che utilizza: questo fatto costringe a dare diritti amministrativi anche a chi non ha competenze specifiche. Nell'allegato "ListaAmministratori" è mantenuto un elenco aggiornato degli utenti con diritti amministrativi sul PC client.	M	ListaAmministratori.ods 2017-09-28 11:26:10
5	1	2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato	L'utilizzo della possibilità di accedere con credenziali amministrative è lasciato alla discrezionalità dell'utente cui spetta la gestione amministrativa della macchina e/o del sistema. Tuttavia, qualora fosse effettuato l'accesso con credenziali amministrative locali o di sistema, questo viene registrato sul log di sistema e centralmente tramite 'System Log'.	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
5	1	3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa	Questo punto è gestito tramite l'utilizzo di 'Active Directory' che permette la creazione di utenti con diversi gradi di autorizzazioni e, di conseguenza, la possibilità di accedere alle impostazioni di sistema in relazione alla loro necessità	S	
5	2	1	Mantenere l’inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata	Questo punto è gestito tramite 'Active Directory' e policy di Windows. In particolare, dall' 'Active Directory' è possibile ricavare l'elenco degli amministratori di dominio; da policy, invece, viene aggiornata ogni giorno la lista degli utenti amministratori delle PdL. In allegato l'elenco degli amministratori. //DA FARE	M	ListaAmministratori.ods 2017-09-28 11:26:41
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	Questo punto è gestito dal personale dell'ufficio manutenzione software e hardware che si occuperà di inizializzare la macchina con gli accessi necessari all'utente cui spetterà l'utilizzo della macchina cancellando altre forme di accesso	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
5	4	1	Tracciare nei log l’aggiunta o la soppressione di un’utenza amministrativa	//DA FARE Questo punto è gestito tramite 'Active Directory' che si occupa di mantenere sempre aggiornata la lista di utenti a cui sono cosentiti i privilegi di amministratore, che si suddividono in amministratori locali, cioè riferibili ad una particolare PdL -Postazione di Lavoro-, e quelli di sistema, che invece fanno riferimento al dominio. Sono settate delle policy Windows per le quali giornalmente viene aggiornata, se necessario, la lista degli utenti amministratori	S	
5	4	2	Generare un’allerta quando viene aggiunta un’utenza amministrativa	//DA FARE Questo punto è gestito tramite 'Active Directory'. Può essere settato un'impostazione per la quale vengono avvisati i responsabili dell'ufficio 'Manutenzione e Gestione Hardware/Software' dell'ufficio CED della PA Provincia di Treviso	S	
5	4	3	Generare un’allerta quando vengano aumentati i diritti di un’utenza amministrativa	//DA FARE Questo punto è gestito tramite 'Active Directory'. Può essere settato un'impostazione per la quale vengono avvisati i responsabili dell'ufficio 'Manutenzione e Gestione Hardware/Software' dell'ufficio CED della PA Provincia di Treviso	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
5	5	1	Tracciare nei log i tentativi falliti di accesso con un’utenza amministrativa	//DA FARE Questo punto è gestito tramite 'Active Directory'. Può essere tenuta traccia dei tentativi di log falliti da parte di un'utenza amministrativa locale o di sistema che possono rappresentare un tentativo di accesso non consentito da parte di utenti privi di permessi o di problemi interni alla rete	S	
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)	Questo punto è gestito tramite 'Active Directory' che impedisce la creazione di utenti (amministratori e non) con una password inferiore ai caratteri minimi richiesti (14 caratteri). //DA MODIFICARE	M	
5	7	2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli	Questo punto è gestito tramite 'Active Directory' che impedisce la creazione di utenti con una password inferiore ai caratteri minimi richiesti per una maggiore sicurezza. In merito al cambio password, vengono utilizzate delle policy Windows che richiedono dei criteri di sicurezza minimi specifici per cui la password possa essere ritenuta valida. In particolare per le utenze amministrative la password dovrà essere più complessa per garantire una maggiore protezione del sistema	S	
5	7	3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)	Questo punto è gestito tramite policy Windows per le quali ogni 45 giorni viene richiesto un cambio password con le caratteristiche minime di sicurezza – Lunghezza: 14 caratteri; 1 lettera maiuscola; 1 numero	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
5	7	4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history)	Questo punto è gestito tramite policy Windows per cui non è possibile utilizzare una password che sia stata utilizza precedentemente. Viene mantenuto uno storico delle 5 password utilizzate in precedenza rispetto a quella attuale	M	
5	7	5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova	Questo punto è gestito tramite policy Windows per le quali ogni 45 giorni viene richiesto un cambio password con le caratteristiche minime di sicurezza – Lunghezza: 8 caratteri; 1 lettera maiuscola; 1 numero; 1 carattere speciale	S	
5	7	6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi	Questo punto è gestito tramite policy Windows che impediscono il riutilizzo delle stesse credenziali di accesso scelte nei 6 mesi precedenti. Ciò è permesso perchè viene mantenuto uno storico delle password (password history)	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	// QUESTO PUNTO AL MOMENTO NON VIENE GESTITO scrivere gestione manuale	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	// QUESTO PUNTO AL MOMENTO NON VIENE GESTITO macchina che raccogli e i log	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
5	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse	Sui client, l'utente può avere anche ruoli amministrativi (vedi punto 5.2.1), quindi non vi è una vera distinzione tra utenza privilegiata e non. L'amministrazione dei server viene effettuata con utenze amministrative "personali", che agiscono con i privilegi di amministratore di dominio.	M	
5	10	2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona	A ogni utente amministratore viene assegnato uno specifico username irripetibile all'interno del sistema a cui corrisponde una password. Entrambi sono incedibili e strettamente personali. //IMPLEMENTARE QUESTA POLITICA ANCHE PER SERVER LINUX	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	//DA IMPLEMENTARE SU SISTEMI LINUX. Questo punto è a discrezione dell'utente cui spetta la gestione amministrativa della macchina e/o dell'intero sistema. Tuttavia, quando viene effettuato l'accesso tramite credenziali amministrative locali o di sistema, viene registrato tramite 'System Log'. Ciò garantisce di sapere chi ha effettuato l'accesso, dal momento che le credenziali sono nominali, e in che momento	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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)	La rete della PA Provincia di Treviso prevede la possibilità all'interno del proprio sistema dell'esistenza di utenti con privilegi di amministratore locale per concedere la possibilità di installare software all'interno della macchina utilizzata. E' a discrezione dell'utenza non utilizzare credenziali di amministratore locale nelle macchine dedicate ad attività che prevedono l'utilizzo di livelli più alti di amministrazione	S	
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza	Queste (credenziali di root per sistemi Linux ed administrator per sistemi Windows) vengono conservate dal responsabile del settore sistemi informatici, il quale sovraintende al loro utilizzo	M	
5	11	2	Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette	Non vengono utilizzati certificati digitali per l'autenticazione.	M	
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	Questo punto è gestito dall'ufficio manutenzione hardware e software tramite immagini di installazione che sono comuni a tutte le macchine connesse alla rete della PA Provincia di Treviso. I programmi base che vengono preinstallati all'interno della macchina prevedono anche l'utilizzo dell'antivirus 'AVG' il quale periodicamente controllerà la presenza di aggiornamenti nella definizione dei virus e li installerà automaticamente	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
8	1	2	Installare su tutti i dispositivi firewall ed IPS personali	Questo punto non viene gestito puntualmente su ogni PdL ma garantito dalla presenza di firewall di frontiera Da verificare con Ezio	M	
8	1	3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati	Questo punto è gestito tramite 'AVG Admin Console' che monitora costantemente la situazione delle macchine su cui è preinstallato l'antivirus 'AVG', prerequisito necessario perchè tale monitoraggio possa funzionare. Mettere insieme le info su attacchi esterni (vedi Admin Exile)	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	Questo punto è gestito tramite 'AVG Admin Console' che monitora costantemente la situazione delle macchine	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	Questo punto è gestito tramite 'AVG Admin Console'. Ogni unità connessa alla rete della PA Provincia di Treviso ha preinstallato al proprio interno l'antivirus 'AVG'. E' possibile eseguire un aggiornamento automatico dell'antimalware. Dalla console, inoltre, è possibile verificare se nella macchina è presente l'ultima versione del prodotto e il corretto funzionamento dello stesso	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
8	3	1	Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali	Questo punto è gestito tramite l'utilizzo di password che impediscono l'accesso ai mezzi dotati di ricevitori wifi di coloro che sono ospiti della struttura. Inoltre, è a discrezione dell'utenza non inserire all'interno della rete della PA Provincia di Treviso strumenti che non siano strettamente necessari per funzioni lavorative e che potrebbero presentare problemi di vulnerabilità: qualora ciò avvenisse (entro le 24 ore) la porta ethernet viene automaticamente disabilitata sullo switch	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	Questo punto è gestito tramite sistema operativo 'Windows'. L'ufficio 'Manutenzione e Gestione Hardware/Software' si occuperà di configurare il SO -sistema operativo- prima della consegna della macchina all'utente. Questo è possibile in quanto Microsoft ha previsto dei tools -strumenti- interni per la gestione delle vulnerabilità previste dal punto 8.4.1. Per una descrizione più dettagliata di tali strumenti si rimanda ai link di riferimento Confronto con Gaetano Sosero	S	
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	Questo punto è gestito tramite firewall di sistema 'SonicWall' che si occupa di monitorare in tempo reale e a filtrare automaticamente i dati proveniente dall'esterno verso i sistemi della PA Provincia di Treviso	S	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
8	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione	Questo punto è gestito tramite l'utilizzo di un server proxy e firewall 'SonicWall' dotato di sistema di filtraggio dei dati, basandosi su blacklist di contenuti e siti web malevoli. Devono essere presenti anche azioni di ripiego (e.g. Reindirizzamento ad un sito prestabilito al momento di rilevazione di malware)	S	
8	7	1	Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili	Questo punto è gestito per mezzo di policy Windows in cui viene bloccata l'esecuzione automatica -Autoplay- delle periferiche removibili che vengono connesse all'utenza	M	
8	7	2	Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file	Questo punto è gestito tramite policy Windows per mezzo della disabilitazione delle estensioni web che prevedono il caricamento di questo tipo di contenuti	M	
8	7	3	Disattivare l’apertura automatica dei messaggi di posta elettronica	Questo punto è gestito tramite l'utilizzo di un particolare webclient -Horde World Group Mail- che non prevede l'apertura automatica delle email che vengono ricevute. Altri client di posta elettronica non possono essere gestiti secondo queste modalità di funzionamento, quindi non sono ammissibili	M	
8	7	4	Disattivare l’anteprima automatica dei contenuti dei file	Questo punto è gestito tramite policy Windows che permettono la disattivazione dell'anteprima dei file	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
8	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione	Questo punto è gestito tramite l'antivirus 'AVG' presente in ogni macchina connessa alla rete della PA Provincia di Treviso. Nelle impostazioni dell'antivirus viene resa standard la scelta di eseguire automaticamente una scansione malware al rilevamento di una nuova periferica rimovibile DA VERIFICARE CON EZIO	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	Questo punto è gestito tramite l'utilizzo di un particolare webclient - Horde World Group Mail- munito di filtri antispam (ClamAV) e di una blacklist in base alla quale concedere l'inoltro alla casella di posta in arrivo della email in questione	M	
8	9	2	Filtrare il contenuto del traffico web	Questo punto è gestito tramite l'utilizzo di un server proxy e del firewall 'SonicWall' dotato di sistema di filtraggio dei dati, basandosi su blacklist di contenuti e siti web malevoli. Cercando di navigare in domini non consentiti, si viene reindirizzati ad una pagina preestabilita che avvisa della rilevazione di malware	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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)	Questo punto è gestito tramite l'utilizzo di un server proxy/firewall dotato di sistema di filtraggio dei dati, basandosi su blacklist di contenuti e siti web malevoli. Devono essere presenti anche azioni di ripiego (e.g. Reindirizzamento ad un sito prestabilito al momento di rilevazione di malware). Per quanto concerne la posta, si utilizza un server mail -Horde World Group Mail- che prevede il filtraggio automatico delle email in relazione a specifici filtri e blacklist di domini spam	M	
8	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento RICERCA DA FARE SU AVG	Questo punto è gestito tramite 'AVG Admin Console' che monitora costantemente la situazione delle macchine su cui è preinstallato l'antivirus 'AVG', prerequisito necessario perchè tale monitoraggio possa funzionare DA CHIEDERE AD EZIO per AVG	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	Lo fa AVG Admin Console secondo una procedura manuale	S	

ABSC_ID			Descrizione	Implementazione	Livello	Link/Allegati
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema	Questo punto è gestito automaticamente per mezzo del server storage IBM Tivoli che riceve le copie di tutti i file che vengono creati, modificati o cancellati dalle varie utenze presenti nella rete della PA Provincia di Treviso. Ogni utenza è configurata perchè giornalmente mandi i suoi contenuti a questo server. Il server poi si occuperà di salvarli all'interno di specifiche 'cassette' che costituiscono il supporto fisico per il backup. Tivoli mantiene 3 copie di uno stesso file per garantire la reperibilità di un'altra copia in caso di corruzione di una di esse. Qualora un file dovesse venire cancellato da un' unità, il server manterrà le copie dello stesso per un periodo di 4 mesi	M	
10	2	1	Verificare periodicamente l’utilizzabilità delle copie mediante ripristino di prova	Questo punto è gestito dal personale dell'ufficio 'Manutenzione e Gestione Software/Hardware' che ha il compito di monitorare lo stato di salute del server IBM Tivoli dove sono caricate le varie copie dei file che vengono prodotti all'interno della rete PA Provincia di Treviso	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	Questo punto è gestito automaticamente per mezzo del server storage IBM Tivoli che effettua una “criptazione” dei dati ricevuti dalle macchine di tutta la PA Provincia di Treviso. Tali dati saranno accessibili soltanto da apposito client	M	

	ABSC_ID		Descrizione	Implementazione	Livello	Link/Allegati
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	Questo punto è garantito dal fatto che periodicamente viene estratta una cassetta dal sistema di backup IBM Tivoli e viene conservata offline	M	
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	Questo punto è gestito dal responsabile dell'ufficio che produce le informazioni tramite il blocco dell’accesso alle informazioni riservate (da procedura informatica)	M	
13	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Il sistema IBM Tivoli su cui vengono salvate le copie di sicurezza dei dati prodotti dall'intero ente pubblico vengono criptati automaticamente dal sistema	S	
13	8	1	Bloccare il traffico da e verso url presenti in una blacklist	Questo punto è gestito tramite l'utilizzo di un server proxy e firewall 'SonicWall' dotato di sistema di filtraggio dei dati, basandosi su blacklist di contenuti e siti web malevoli. Devono essere presenti anche azioni di ripiego (e.g. Reindirizzamento ad un sito prestabilito al momento di rilevazione di malware)	M	