ALLEGATO 21

allegato 13

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
1	1	1	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Min.	Lo stato attuale della ASST prevede la presenza di un inventario relativo alle PdL gestite tramite il servizio di Fleet Management denominato CA Service Desk Manager. Il sw permette di tracciare e gestire tutti gli apparecchi in manutenzione. Sono attualmente escluse tutte le apparecchiature non di diretta competenza del servizio Fleet. Al fine di strutturare un inventario delle risorse attive è in corso di valutazione uno strumento di scansione della rete in grado di recepire e catturare tali risorse. Questa soluzione permetterebbe di concentrare in un'unica piattaforma le informazioni relative ai dati identificativi (IP, MAC address, nome, etc...) degli apparati di rete. Data la natura eterogenea di tali apparati tale inventario dovrà necessariamente essere popolato dalle informazioni puntuali reperibili dai vari sottosistemi quali: apparecchiature elettromedicali, apparecchi telefonici, sistemi di videosorveglianza, infrastruttura di rete, sistemi di allarme antintrusione e antincendio, monitoraggi ambientali. Per quanto riguarda i dispositivi medici gestiti dall'Ingegneria Clinica collegati alla rete, seguono essenzialmente due politiche. Apparecchi che hanno necessità di indirizzamenti riservati e apparecchi che possono lavorare in DHCP. Nella prima categoria rientrano in generale apparecchiature (quali TAC, RM, etc...) che per loro natura hanno necessità di una connessione stabile e definita con sistemi esterni quali potrebbero essere ad esempio sistemi di archiviazione immagini, RIS, sistemi server. Nella seconda categoria invece rientrano apparecchi di vario genere che non hanno esigenze restrittive in caso di connettività di rete. In queste categoria rientrano ad esempio sistemi di monitoraggio di parametri ambientali che effettuano un invio di dati ai sistemi di centralizzazione. Le apparecchiature che vengono collegate alle VLAN per le quali è prevista la reservation degli indirizzi vengono associate mediante MAC ADDRESS degli strumenti stessi. E' previsto per questi casi che l'ingegneria clinica richieda tramite il sistema di tracciabilità di ticketing (CA Service Desk Manager) ai sistemi informativi dell'azienda l'attivazione delle prese, segnalando di quale tipologia di apparecchio si tratti dandone una breve descrizione e l'indirizzo fisico della macchina. Attualmente gli apparecchi che vanno in rete con DHCP invece non vengono tracciati qualora non si renda necessaria la reservation. Al fine invece di tenere traccia anche di tali apparecchiature verrà utilizzato il sistema di ticketing. Dall'inventario sono escluse le reti pubbliche di accesso che registrano solo il MAC address dell'apparecchio che si connette. Le reti pubbliche sono separate dalle reti aziendali tramite Firewall e le attività di ciascun apparecchio collegatosi alla rete pubblica viene tracciato dai log del firewall stesso.	2017
1	1	2	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Std.	Al fine di strutturare un inventario delle risorse attive è in corso di valutazione uno strumento di scansione della rete in grado di recepire e catturare tali risorse. Questa soluzione permetterebbe di concentrare in un'unica piattaforma le informazioni relative ai dati identificativi (IP, MAC address, nome, etc...) degli apparati di rete e di ricevere allarmi in caso di anomalie	2018
1	1	3	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Alto	lo strumento di scansione della rete in corso di valutazione sarà in grado di effettuare il discovery dei dispositivi collegati alla rete e di inviare allarmi in caso di anomalie	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
1	1	4	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Alto	Al momento implementato solo per quanto riguarda la quantità di banda utilizzata. Il software in corso di valutazione, per poter essere acquisito, dovrà poter qualificare i sistemi connessi attraverso l'analisi del traffico.	2018
1	2	1	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Implementare il "logging" delle operazioni del server DHCP.	Std.	nei log del dhcp server sono riportate date e ora delle richieste associandole al mac address del client	2018
1	2	2	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Std.	Per la valutazione, attualmente in corso, del software di discovery si tiene in considerazione la necessità di poter integrare dati esterni (provenienti dal DHCP server) per un miglior inventario	2018
1	3	1	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Min.	Il sistema di ticketing per comunicare la necessità di collegamento in rete di apparecchiature di qualsiasi natura consente di tracciare e mantenere aggiornabile l'inventario delle risorse attive quando sarà implementato il sistema di scansione automatico della rete aziendale. Questo sistema di comunicazione è attualmente attivo per lo scambio di informazioni tra SIA e Ingegneria Clinica a cui si aggiunge la Fondazione MBBM.	2017
1	3	2	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Std.	Per la valutazione, attualmente in corso, del software di discovery si tiene in considerazione la necessità di dover avere un inventario sempre aggiornato automaticamente	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
1	4	1	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Min.	Il DHCP server aziendale di ASST Monza gestisce la distribuzione degli indirizzi IP e quindi è sempre aggiornato automaticamente con tutti gli IP presenti in rete. Per apparecchiature dell'ingegneria Clinica che non sono windows based ma acquisiscono IP dinamicamente i dettagli sono estraibili da DHCP tramite mac address. E' in corso di valutazione la possibilità di tracciare al momento della fornitura di apparecchi elettromedicali, i dati identificativi della connettività di rete quali: nome macchina, MAC address e tipo di indirizzamento richiesto. In tal caso tali dati sarebbero riportati nel sistema gestionale del fornitore del servizio di Global Service che attualmente è gestito tramite il fornitore Tecnologie Sanitarie e la piattaforma sw Cosvin. Gli apparecchi che si connettono a rete pubblica non sono gestiti in quanto non inventariati ma la loro attività è tracciata tramite log. Il software Imc si affianca al dhcp server aziendale e rileva, insieme a tutti gli gli indirizzi ip (dinamici o statici) e mac address connessi alla rete, l'esatta posizione per una puntuale e precisa collocazione all'interno della struttura.	2017
1	4	2	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	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.	Std.	Per tutti i dispositivi che possiedono un indirizzo IP è possibile un inventario che indica i nomi delle macchine attraverso il server dhcp ed il server Imc. In active directory, invece, è rintracciabile la funzione del sistema, il titolare responsabile della risorsa e l'ufficio associato, se il dispositivo è fisico o virtuale, se è portatile o fisso. Il software in corso di valutazione deve, per poter essere acquisito, rispondere a queste esigenze	2018
1	4	3	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	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.	Alto	I dispositivi che memorizzano o elaborano dati sono sempre identificati, sia essi telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili, perché l'attività di connessione al dominio o di configurazione per l'accesso ai dati è sempre eseguita a fronte di un ticket e quindi registrata	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
1	5	1	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	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.	Alto	questo progetto è stato inserito, quindi è oggetto di discussione, nelle richieste all'attuale gestore dell'infrastruttura	2019
1	6	1	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale	Alto	questo progetto è in fase di valutazione, al momento a livello di indagine.	2019
2	1	1	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	Stilare 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. Non consentire l'installazione di software non compreso nell'elenco.	MIn.	sui sistemi server vengono installati esclusivamente sw di produttività aziendale (db e applicativi) regolarmente licenziati. tutti questi software sono censiti. Nell'ambito delle attività di competenza del Fleet Management i software standard adottati nell'ASST sono censiti, con riferimenti relativi al produttore, di escalation e procedure di installazione. Nell'ambito di tali software rientrano non solo i pacchetti sw di produttività personale ma anche i sw di uso comune nelle attività lavorative dell'azienda. L'elenco dei sw autorizzati, sia per sistemi client che per sistemi server, è stilato dal responsabile del SLA e inviato (per la parte client) al servizio di Fleet. Di tutti i software commerciali vengono effettuati controlli relativi al regolare possesso delle licenze. Gli utenti hanno generalmente privilegi di user sui client e per l'installazione di qualunque applicativo devono effettuare richiesta tramite sistema di ticketing al SIA, che ne dà autorizzazione. Dell'elenco non fanno parte i software a corredo delle apparecchiature intesi come stand alone ed essenziali al corretto funzionamento dell'apparecchiatura stessa. Ovvero tutti quei sw che pur essendo installati su pc collegati alla rete non necessitano di condivisioni o di comunicazioni verso server.	2017
2	2	1	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	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.	Std	I software non inclusi nella whitelist sono in costante aggiornamento e oggetto di revisione. è in fase di studio un progetto per poter gestire i blocchi dei software non autorizzati	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
2	2	2	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	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).	Std.	è in fase di studio un progetto per poter gestire i blocchi del software non autorizzati e per poter creare delle whitelist configurabili e personalizzabili a seconda del profile dell'utente o della postazione di lavoro	2019
2	2	3	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Alto	è in fase di indagine la ricerca di un software o di strumenti che possano soddisfare tale richiesta	2019
2	3	1	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Min.	il software o i sistemi che si stanno cercando dovranno necessariamente avere la possibilità di rilevare presenza di software non autorizzato	2018
2	3	2	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Std.	sarà predisposto un documento (qualità) con un inventario del software e le relative procedure per mantenerlo aggiornato	2018
2	3	3	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	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.	Alto	la soluzione non è al momento presente ma è oggetto di studio. Nel corso dei prossimi incontri sarà inserito nell'o d.g. la ricerca di una soluzione adeguata	2018
2	4	1	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	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.	Alto	al momento non si è ancora resa necessaria nessuna procedura di isolamento ma siamo predisposti, con la segmentazione in vlan e ambienti virutali separati, per poter creare vm air gapped i soli casi presenti in ASST Monza di sistemi air gapped sono relativi a sistemi di ingegneria clinica, per cui non virtualizzabili perché connessi direttamente a strumenti esterni.	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
3	1	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Min.	I sistemi vengono installati utilizzando immagini (fisico) o template (virtuale) che adottano configurazioni sicure	2018
3	1	2	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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.	Std.	Sull'immagine dei client distribuita e nei template dei server gli account non necessari, compresi gli account di servizio, sono stati eliminati. Il software installato e distribuito con l'immagine è solo quello di ampia adozione in Azienda, necessario per garantire la continuità lavorativa degli Operatori Sanitari che si muovono tra reparti. I componenti di sistema non necessari sono stati rimossi ed i servizi e le operazioni pianificate di Windows non necessarie sono state disabilitate	2018
3	1	3	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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.	Alto	Le immagini dei client e i template dei server vengono regolarmente aggiornati sia per questioni di sicurezza e sia per ridurre i tempi di attesa in fase di configurazione di nuovi server o pdl	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
3	2	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Min.	le configurazioni hardware e l'installazione del sistema operativo vengono svolte seguendo una precisa reference architecture. la configurazione hardware (firmware e bios) da remoto è gestita solo sui server esclusivamente dagli amministratori della sala macchine grazie all'utilizzo di switch di management separati dalla rete dati. Per i client, stampanti e altri tipi di sistema la configurazione viene eseguita dai tecnici del fleet management prima dell'inizio dell'installazione delle immagini. Per la parte client è presente un layout ben definito dell'immagine e delle componenti in essa installati. E' disponibile un changelog in cui vengono riportate le modifiche effettuate ad ogni aggiornamento. Per le VM dell'ambiente virtuale sono disponibili i template da cui partire per la creazione di nuovi server per tutti i sistemi operativi tipo server autorizzati. I server fisici sono tutti in cluster. In questo caso il sistema operativo arriva installato e le configurazioni hardware sono impostate dal produttore che deve intervenire anche in caso di reinstallazione con i supporti a corredo. A tutte le immagini ed i template vengono applicate le procedure di hardening. I dispositivi medicali di competenza SIC (quando forniti di HW quali laptop, desktop, etc...) vengono forniti con software embedded. Tutti i dispositivi con marcatura CE vengono forniti con le impostazioni di fabbrica e non vengono modificati.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
3	2	2	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Min.	In caso di compromissione si procede alla categorizzazione dell'incidente e alla valutazione della situazione e si opera, sulla base dei possibili scenari prospettati, nelle varie modalità previste. Solitamente, in caso di compromissione del client, la pdl viene ritirata e portata in laboratorio e inserita in lan separata per un'analisi senza rischi. In caso di ripristino totale il pc viene riconfigurato utilizzando l'immagine hardened. Anche per i server dell'ambiente virtuali, in caso di compromissione, è prevista una analisi della situazione per valutare costi/benefici e possibili scenari prospettati a seconda delle varie modalità di intervento applicabili. In caso di ripristino dell'intero sistema è possibile utilizzare, oltre al template hardened, anche l'immagine salvata, nata da una configurazione standard, in uno dei giorni precedenti dopo il relativo controllo e scansione da console di antivirus. Per i server fisici, in caso di compromissione, si procede al ripristino sia delle configurazioni iniziali che del sistema operativo con i supporti a corredo. In questo caso il carico di lavoro viene spostato sul secondo nodo del cluster e si lavora off-line sul server compromesso.	2017
3	2	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Std.	L'immagine dei client viene aggiornata a seguito di una specifica richiesta di uno dei fornitori (tracciata con ticket Imac) o in seguito ad una modifica dell'hardware in fornitura (sempre con ticket) sempre sotto la supervisione e responsabilità del S.I.A.. In caso di modifica dell'immagine e del template vengono applicati contestualemente tutti gli aggiornamentei di sicurezza e dell'antivirus. Nel caso in cui, per una anno, non si sia mai presentata la necessità di aggiornare una immagine o un template, si procede comunque alla creazione di nuovi supporti con gli aggiornamenti di sistema operativo (sicurezza e critici) e di antivirus.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
3	3	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Le immagini d'installazione devono essere memorizzate offline.	Min.	L'immagine dei client viene conservata su dispositivi off-line all'interno dell'ufficio tecnico del presidio, dove è custodita all'interno di un cassetto chiuso a chiave e l'ufficio stesso è dotato di sistema di allarme. Una copia è presente su pc di laboratorio separato dalla rete per velocizzare le operazioni in periodi di alto carico di lavoro. Per i server fisici i supporti di reinstallazione sono conservati all'interno dell'ufficio tecnico del presidio, dove è custodita all'interno di un cassetto chiuso a chiave e l'ufficio stesso è dotato di sistema di allarme. Per i server virtuali i template sono inseriti in una lun di uno storage in fibra accessibile esclusivamente dagli amministratori della sala macchine (sia dal punto di vista fisico che via remota). Per il futuro si sta organizzando un sistema di gestione dei template offline.	2017
3	3	2	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Std.	L'immagine dei client viene creata all'interno dell'ufficio tecnico del presidio, dove è custodita all'interno di un cassetto chiuso a chiave e l'ufficio stesso è dotato di sistema di allarme. L'integrità dell'immagine viene controllata 2 volte al mese e ogni 2 mesi avviene la verifica dell' hash del file immagine. Per i server fisici i supporti di reinstallazione sono conservati all'interno dell'ufficio tecnico del presidio, dove sono custoditi all'interno di un cassetto chiuso a chiave e l'ufficio stesso è dotato di sistema di allarme. Per i server virtuali i template sono inseriti in una lun di uno storage in fibra accessibile esclusivamente dagli amministratori della sala macchine (sia dal punto di vista fisico che via remota). Il controllo dell'integrità al momento non è gestito ma stiamo valutando, con il fornitore del fleet management, l'implemetazione di un software con funzione di verifica e confronto dei valori hash o checksum con diversi algoritmi	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
3	4	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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).	Min.	L'amministrazione remota dall'esterno dell'Azienda può avvenire solamente tramite VPN con certificati rilasciati dall'Ente o via tunnel Ipsec. Internamente alla LAN solamente le utenze autorizzate sono in grado di autenticarsi su server e client. Per i sistemi server microsoft la connessione avviene quasi esclusivamente via rdp. Le poche eccezioni esistenti sono documentate e autorizzate dal S.I.A. Per i sistemi server Linux la connessione è esclusivamente via ssh. La gestione remota dei client microsoft avviene via vnc con abilitazione ai soli utenti con privilegi amministrativi. Il monitoraggio remoto di apparecchiature elettromedicali (TAC, RM, RIS/PACS,...) avviene tramite connessioni IPSec. La richiesta di connettività avviene tramite sistema di ticketing. La gestione via web dei dispositivi, quali stampanti, avviene con protocollo https dove il sistema lo permette. La gestione remota dell'infrastruttura sta migrando verso l'utilizzo di ssh dove il sistema lo permette. La connettività remota verso il presidio di Desio viene gestito dalla ASST di Vimercate in quanto a seguito della LR 23/2015 le due aziende hanno mantenuto la gestione separata delle reti. Tra ASST Brianza e ASST Vimercate così come con ATS Brianza sono state predisposte delle VPN da provider per consentire la comunicazione di alcune sottoreti definite tramite natting. Le tabelle di natting sono state definite e concordate dai Responsabili dei rispettivi Servizi Informativi.	2017
3	5	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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.	Std	al momento non è implementato ma è inserito nell'o.d.g. dei prossimi incontri strategici.	2019
3	5	2	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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.	Alto	Il sistema che verrà adottato dovrà necessariamente poter generare degli alert automaticamente in caso di alterazione dei file.	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
3	5	3	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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.	Alta	il sistema che verrà adottato dovrà necessariamente essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica	2019
3	5	4	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle	Alta	il sistema che verrà adottato dovrà necessariamente essere in grado di identificare le alterazioni sospette	2019
3	6	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Alta	al momento non è implementato ma è inserito nell'o.d.g. dei prossimi incontri strategici.	2019
3	7	1	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Alta	essendo un progetto ancora in fase progettuale, verrà studiato un sistema che possa gestire sia le modifiche non autorizzate e sia quelle autorizzate e che possa ripristinare le impostazioni	2019
4	1	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	Min	essendo un progetto ancora in fase progettuale, verrà studiato un sistema che possa gestire una ricerca delle vulnerabilità e delle relative criticità	2019
4	1	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4 1 1 con frequenza commisurata alla complessità dell'infrastruttura.	Std	il sistema che verrà adottato dovrà necessariamente essere utilizzato con frequenza commisurata all'infrastruttura e alla sua complessità	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
4	1	3	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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).	Alto	al momento non è implementato ma è un argomento su cui ci si confronterà e che sarà oggetto di studio.	2019
4	2	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Std.	volendo individuare uno SCAP da utilizzare sarà inserito, tra i requisiti minimi richiesti, la possibilità di poter correlare i propri dati con informazioni esterne	2019
4	2	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità.	Std.	quando sarà implementato un sistema di ricerca delle vulnerabilità si creeranno delle procedure e/o automazioni per la verifica richiesta	2019
4	2	3	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Std.	quando sarà implementato un sistema di ricerca delle vulnerabilità si creeranno delle procedure e/o automazioni per la verifica richiesta	2019
4	3	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	Std.	quando sarà implementato un sistema di ricerca delle vulnerabilità si creeranno delle utenze privilegiate da utilizzare esclusivamente per queste attività	2019
4	3	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	Std.	quando sarà implementato un sistema di ricerca delle vulnerabilità si creeranno delle procedure e regole e si farà formazione per il relativo utilizzo	2019
4	4	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Min.	quando sarà implementato un sistema di ricerca delle vulnerabilità si creeranno delle procedure e regole per mantenere aggiornati i sistemi	2019
4	4	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Std.	in fase di acquisizione dello strumento di scansione delle vulnerabilità sarà indispensabile la registrazione ad un servizio con questi requisiti.	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
4	5	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Min.	Relativamente ai sistemi client e server l'aggiornamento avviene tramite i rispettivi repository (Microsoft WSUS / Redhat Yum Repositories). I client installano automaticamente gli aggiornamenti rilasciati da Microsoft Wsus previa approvazione degli amministratori di dominio. Per i pc di utenti sanitari il riavvio è a discrezione dell'utilizzatore, in quanto un riavvio automatico potrebbe creare disagio durante un momento critico con un paziente L'aggiornamento dei server e dei domain controller è effettuata mensilmente dagli amministratori della sala macchine in orari studiati per recare il minimo disagio possibile. In corso di formalizzazione la procedura già in uso. Gli aggiornamenti delle applicazioni vengono rilasciati dai fornitori e generalmente vengono propagate sui client a livello centralizzato con strategie variabili in base all'applicazione (Software Distribution, script di avvio dell'applicazione, ecc...).	2017
4	5	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità	Min.	Apparecchiature dotate di software a corredo ma isolate dalla rete informatica sono sottoposte alle normali operazioni di manutenzione definite dal costruttore dell'apparecchio e previste dalle normative relative alle apparecchiature elettromedicali. Generalmente non sono previsti contrattualmente aggiornamenti software poiché questi sono strettamente correlati all'hardware utilizzato in seguito alla certificazione CE come Dispositivo Medico. La contrattualizzazione di un aggiornamento dovrebbe quindi prevedere adeguamenti sia hardware che software che potrebbero comportare la sostituzione totale dell'apparecchiatura stessa. Questo a fronte, ad esempio, di apparecchiature il cui ciclo di vita all'interno della struttura può essere di svariati anni ben oltre al ciclo di vita normale di un comune pc.	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
4	6	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite	Std.	quando sarà implementato un sistema di ricerca delle vulnerabilità le utenze privilegiate svolgeranno queste attività secondo policy predefinite	2019
4	7	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	Min.	quando sarà implementato un sistema di ricerca delle vulnerabilità verranno anche stilate le procedure di remediation o di intervento	2019
4	7	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	Std.	I server vengono aggiornati costantemente e i relativi software (gestiti dai fornitori) devono essere sempre conformi. Relativamente all'immagine dei client viene risolutato ad ogni aggiornamento in tutti l'aggiornabili dei singoli componenti se, tenendo conto della compatibilità con le applicazioni distribuite i server vengono aggiornati costantemente, in collaborazione (dove serve) con il fornitore, per mantenere controllato il livello di rischio	2019
4	8	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.)	Min.	sarà definito, a seguito dell'utilizzo di un software di scansione, un piano di gestione dei rischi	2019
4	8	2	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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	Min.	sarà definito, a seguito dell'utilizzo di un software di scansione, un piano di intervento per la risoluzione nella modalità richiesta	2019
4	9	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	Prevedere, in casi 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.	Std.	insieme al piano di intervento per la risoluzione delle criticità verrà redatto anche un documento contenente misure alternative	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
4	10	1	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	Std.	a tutti i nostri fornitore è stato messo a disposizione un ambiente di test di macchine virtuali dove fare le prove degli aggiornamenti/modifiche prima di installare sui server di produzione. Per i sistemi in gestione di Ingegneria Clinica viene richiesto ai diversi fornitori di sviluppare e testare eventuali soluzioni personalizzate in ambiente di test messo a disposizione dalla ASST. In particolare tali richieste vengono formalizzate a partire dall'eventuale Capitolato di Appalto della fornitura.	2017
5	1	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	MA.	In ASST Monza gli unici ad avere privilegi di amministrazione sono: - componenti del s.i.a. che si occupano di assistenza o del supporto agli applicativi; - componenti del s.i.c che si occupano di assistenza o del supporto agli applicativi; - componenti della fondazione MBBM che si occupano di assistenza o del supporto agli applicativi; - fornitori di applicativi; tutte queste persone hanno sia le competenze che la necessità operativa per essere amministratori (per contratto di assunzione o per contratto di acquisto). all'elenco precedente si aggiungono alcuni utenti che, per comprovata necessità e a seguito di un processo autorizzativo, devono poter utilizzare il pc con privilegi amministrativi	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	1	2	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Min.	Sia sui client che sui server è attivo il logging e la UAC di windows quindi sono reperibili sia le informazione di login e logout e sia le operazioni per cui sono state necessarie le autorizzazioni da amministratore.	2017
5	1	3	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Std.	Al termine di una analisi e una previsione del possibile utilizzo delle utenze amministrative, si procede ad una oculata profilazione che, in linea generale, è organizzata in tre aree: Gli utenti che dispongono di credenziali amministrative devono poter intervenire per installazione e assistenza sui pc e sui server di competenze e quindi vengono abilitati esclusivamente a questi. Così anche i fornitori hanno privilegi amministrativi solo sui server che devono gestire e sulle pdl dove risiede il loro applicativo. Il singolo utente che ha ottenuto l'autorizzazione di essere amministratore del proprio pc ha le credenziali solo per la propria pdl.	2017
5	1	4	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Alta	sia sui client che sui server è attivo il gestore degli eventi ed è configurato il log management sui server. Sarà implemetato uno strumento che consenta di avere lo storico di questi dati da poter analizzare	2019
5	2	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Min.	gli utenti che dispongono di credenziali amministrative sono specificati in base al contratto di assunzione o di acquisto/assistenza ad eccezion fatta per gli utenti amministratori del proprio pc per i quali c'è un ticket di riferimento. È in corso la creazione dell'inventario che, nel corso del tempo, sarà mantenuto aggiornato.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	2	2	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Alto	sarà implementato uno strumento che gestisca le utenze amministrative in maniera automatica	2019
5	3	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Min.	ai server e ai client, prima della connessione alla rete, vengono sostituite le credenziali dell'utenza predefinata con valori coerenti e definite a livello di policy aziendale. Tutte le altre periferiche che prevedono una connessione da remoto (stampanti, videocamere, switch, allarmi, campanelli, ecc.ecc.) hanno modificato, o sono in corso di modifica, le credenziali amministrative. Le utenze di amministrazione locale dei dispositivi elettromedicali sono in generale utilizzate con finalità di service e di esclusivo utilizzo da parte del fornitore/fabbricante.	2017
5	4	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa	Std.	è in corso la verifica della tracciatura, nei log, dell'aggiunta e/o la soppressione di un'utenza amministrativa	2019
5	4	2	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Std.	sarà implementato uno strumento che gestisca le utenze amministrative in maniera automatica e che potrà generare un'allerta in caso di aggiunta	2019
5	4	3	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Std.	sarà implementato uno strumento che gestisca le utenze amministrative in maniera automatica e che potrà generare un'allerta in caso di modifica	2019
5	5	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Std.	è in corso la verifica della tracciatura, nei log, dei tentativi falliti di accesso	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	6	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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.	Alto	al momento non è implementato ma è inserito nell'o.d.g. dei prossimi incontri strategici.	2019
5	7	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Min.	l'applicazione a più fattore non è supportata. Le utenze di dominio con privilegi amministrativi soddisfano il requisito di lunghezza delle pw di 14 caratteri e di robustezza (es. 1 carattere min, 1 carattere maius, 1 numero e/o 1 carattere speciale). Per i dispositivi su cui non è supportata la lunghezza della pw a 14 caratteri, viene utilizzata la lunghezza massima consentita (per es. sistemi quali stampanti o videocamere).	2017
5	7	2	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Std.	le policy di dominio impediscono l'utilizzo di credenziali deboli	2018
5	7	3	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Min.	La regola generale impone una scadenza della pw amministrativa ogni 60 giorni. Sono presenti casi in cui, per comprovata necessità operativa, si è dovuto inibire l'applicazione della policy perché le cedenziali vengono utilizzate da sistemi operativi mission critical. In tali casi viene comunque impedito l'accesso ad internet.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	7	4	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Min.	La password history tiene conto delle ultime 24 utilizzate. La durata minima della password è attualmente impostata a 72 ore. Il cambio o reset della password deve essere richiesto tramite apertura di un ticket al servizio di help desk/fleet management. E' in fase di rilascio un sistema di reset della password tramite associazione dell'utente al proprio numero di cellulare su cui ricevere, al momento della richiesta effettuata tramite web, la password temporanea di accesso.	2017
5	7	5	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova	Std.	La durata minima della password è attualmente impostata a 72 ore.	2018
5	7	6	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Std.	è in fase di modifica la durata minima della password ed della password history	2018
5	8	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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 privile- giato i singoli comandi.	Std.	Viene lasciata attiva di default l'UAC di Windows relativamente ai sistemi operativi che la prevedono. Gli altri sistemi operativi sono classificati come obsoleti e in fase di valutazione la loro sostituzione.	2019
5	9	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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.	Std.	al momento non è implementata ma è inserita nell'o.d.g. dei prossimi incontri strategici.	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	10	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Min.	In azienda gli unici ad avere privilgi di amministrazione sono: - componenti del s.i.a. che si occupano di assistenza o del supporto agli applicativi; è in corso la creazione di una seconda utenza per il personale del s.i.a con privilegi di amministrazione cosi che siano distinte dai profili di utente standard. Questi utenti saranno dotati di una doppia credenziale in AD. - componenti del s.i.c che si occupano di assistenza o del supporto agli applicativi; è in corso la creazione di una seconda utenza per il personale del s.i.c. con privilegi di amministrazione cosi che siano distinte dai profili di utente standard. Questi utenti saranno dotati di una doppia credenziale in AD. - componenti della fondazione MBBM che si occupano di assistenza o del supporto agli applicativi; è in corso la creazione di una seconda utenza per il personale dell fondazione MBBM con privilegi di amministrazione cosi che siano distinte dai profili di utente standard. Questi utenti saranno dotati di una doppia credenziale in AD. - fornitori di applicativi, in questo caso non ha senso fornire una seconda utenza al fornitore che si connette ed opera esclusivamente per assistenza e installazione. - utenti che, per comprovata necessità e a seguito di un ticket con approvazione, devono poter utilizzare il pc con privilegi amministrativi; in questo caso l'utente è, a tutti gli effetti esclusivamente, amministratore di una sola pdl per l'utilizzo quotidiano, non è fattibile fornire a queste persona una seconda utenza e chiedere di disconnettersi e riconnettersi più volta durante il giorno in base al programma in utilizzo.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	10	2	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona	Min.	Tutte le utenze amministrative di personale interno alla ASST sono nominative. Per i fornitori che gestiscono propri sistemi o sistemi di terzi in outsourcing vengono rilasciate delle credenziali con diritti di amministrazione generiche. In generale tali fornitori erogano un servizio di assistenza remota o anche on site basato su una forza lavoro non quantificabile in termini di numero di risorse. In questi casi quindi, non essendo possibile identificare ogni singola persona in grado di effettuare operazioni di assistenza, viene contrattualizzato sin dal CSA il pieno rispetto da parte del fornitore della normativa sulla privacy vigente e dalle indicazioni AgID. Utenze generiche sono attive per ogni reparto e ufficio della ASST ma non hanno alcun tipo di privilegio. Hanno solo diritti di uteriza standard e in generale non accedono a risorse di rete e tutte non possono accederea ad internet.	2017
5	10	3	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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.	Min.	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, sono conservate all'interno dell'ufficio tecnico del presidio, dove sono custodite all'interno di un cassetto chiuso a chiave e l'ufficio stesso è dotato di sistema di allarme. Le password vengono cambiate mensilmente e custodite solo da uno degli amministratori. Vengono utilizzate solamente casi di intervento sui domain controller o sui firewall perimetrali.	2017
5	10	4	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Std.	già predisposto sui sistemi operativi Server. In fase di implementazione sui client.	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
5	11	1	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Min.	Le credenziali di amministratore sono conservate presso la sala macchine del SIA. All'interno dell'area si accede solo tramite lettore di badge i cui accessi sono tracciati e regolamentati (ovvero accedono solo i badge autorizzati). L'area viene allarmata negli orari in cui non è prevista la presenza di personale, l'allarme oltre ad avere un segnale acustico (sirena) viene centralizzato anche presso la centrale operativa della sorveglianza ospedaliera. All'interno dell'area le credenziali sono custodite all'interno di un armadio chiuso a chiave.	2017
5	11	2	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	MIn.	per l'autenticazione non si utilizzano certificati digitali ad esclusione dell'utilizzo del sso che avviene attraverso la tessera CRS ed il relativo pin.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
8	1	1	DIFESE CONTRO I MALWARE	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.	Min.	ASST Monza adotta la soluzione di Sophos denominata "Sophos Endpoint Protection". La soluzione integra una console centralizzata (Sophos Enterprise Console - SEC) di gestione e aggiornamento dei client connessi. L'antivirus è in grado di rilevare le minacce non solo basandosi sul database delle firme integrato, ma anche tramite analisi del comportamento sospetto (HIPS) e rilevamento di traffico malevolo. Inoltre è in grado di rilevare e bloccare malware di classe crypto ransomware analizzando il comportamento sospetto e richieste di connessione a server di generazione della chiave crittografica. I client sono costantemente connessi alla console centralizzata e scaricano i database delle firme aggiornati appena disponibili nell'infrastruttura locale, oltre a riportare alla console centralizzata eventuali minacce rilevate e comportamenti sospetti Per i software delle apparecchiature elettromedicali viene valutato caso per caso la possibilità di utilizzare antivirus. Nei casi in cui sui pc a corredo delle attrezzature sia possibile effettuare l'inserimento nel dominio e l'installazione dell'antivirus aziendale il problema non sussiste. Nei casi in cui invece la certificazione medicale dello strumento non consenta di apportare modifiche alle configurazioni di fabbrica tale installazione non viene effettuata. Va tenuto comunque in considerazione che alcune attrezzature sono spesso dotate di consolle di controllo, queste benchè siano spesso basate su SO Windows non offrono possibilità di accesso se non tramite i tool di service in uso esclusivo all'assistenza del fornitore. In altri casi si può trattare di strumentazione che pur acquisendo indirizzi di rete hanno sistemi proprietari. In ogni caso le apparecchiature in rete non inserite in dominio non possono effettuare navigazione verso l'esterno e non accedono alle risorse di rete condivise.	2017
8	1	2	DIFESE CONTRO I MALWARE	Installare su tutti i dispositivi firewall ed IPS personali.	Min.	Attualmente i client non hanno nessun meccanismo di firewall attivo. Sophos integra un firewall gestito centralmente dalla console dell'antivirus. Anche il sistema operativo in uso ha un firewall gestibile centralmente da policy di dominio. E' in fase di valutazione l'elenco delle regole necessarie al corretto funzionamento delle applicazioni in uso. I test con entrambi i firewall sono già avviati nel laboratorio.	2017
8	1	3	DIFESE CONTRO I MALWARE	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Std.	Attualmente i log dell'antivirus sono archiviati sul server SEC. In azienda è presente un server di log management. In futuro gli eventi rilevati dal SEC saranno registrati nel log management	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
8	3	1	DIFESE CONTRO I MALWARE	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Std.	Il client antivirus è gestito centralmente con la SEC. E' attivo il meccanismo di Tamper Protection che inibisce agli utenti la possibilità di disattivare / disinstallare il client antivirus.	2017
8	3	2	DIFESE CONTRO I MALWARE	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.	Std.	Attraverso una procedura integrata della SEC periodicamente vengono incrociati i client presenti in Active Directory con quelli registrati sulla SEC. I client su cui il Sophos EndPoint Protection non dovesse risultare installato o aggiornato vengono adeguati con modalità push dalla console.	2017
8	3	3	DIFESE CONTRO I MALWARE	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Alto	La soluzione Sophos integra una tecnologia denominata Live Protection. Qualora un client dovesse rilevare un comportamento sospetto, ma non riconducibile ad una minaccia nota, viene effettuata una scansione in cloud sull'infrastruttura di Sophos. E' possibile, per le minacce non riconosciute, anche effettuare il submit di un file sample a Sophos per ulteriori analisi.	2019
8	8	1	DIFESE CONTRO I MALWARE	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Min.	Sophos integra una tecnologia di Device Control che permette di bloccare dispositivi e di gestire eccezioni ai blocchi. Per necessità aziendali non è possibile limitare l'uso di dispositivi esterni su apparecchiature elettromedicali e pdl in quanto a queste deve essere data possibilità di scaricare informazioni per utilizzo a fini clinici o di studio	2017
8	8	2	DIFESE CONTRO I MALWARE	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Alto	Il Device Control di Sophos effettua, quando attivato, logging su SEC dei dispositivi bloccati e di quelli in eccezione.	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
8	4	1	DIFESE CONTRO I MALWARE	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.	Std.	Sull'immagine distribuita è attiva la funzionalità di Data Execution Prevention a livello di Sistema Operativo relativamente a programmi e servizi di Windows. Il client Sophos Endpoint include la funzione "Buffer Overflow Protection Services".	2018
8	4	2	DIFESE CONTRO I MALWARE	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Alta	Attualmente l'unico strumento adottato è il client Sophos Endpoint Protection che è una soluzione completa di sicurezza integrando Antivirus, Anti-malware, firewall, Device Control, Application Control e Data Control.	2019
8	5	1	DIFESE CONTRO I MALWARE	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Std.	la protezione degli host è assicurata da una infrastruttura di ips, poi dai firewall esterni ed infine dai firewall interni	2019
8	5	2	DIFESE CONTRO I MALWARE	Installare sistemi di analisi avanzata del software sospetto.	Alta	Sophos Endpoint Protection, la gestione centralizzata tramite console SEC e la Live Protection in cloud di Sophos, con la possibilità di inoltro di sample file sospetti costituiscono la strategia di analisi avanzata di software sospetto adottata.	2019
8	6	1	DIFESE CONTRO I MALWARE	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Std.	il blocco di accessi a indirizzi con cattiva reputazione è assicurato dal proxy interno e dagli strumenti di analisi ips di rete	2017
8	7	1	DIFESE CONTRO I MALWARE	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Min.	Le funzionalità di autoplay sono disattivate da policy locali sull'immagine dei client attualmente in distribuzione. Analogamente le funzionalità sono disabilitate anche tramite policy di dominio.	2017
8	7	2	DIFESE CONTRO I MALWARE	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file	Min.	Tali funzionalità sono disabilitate da policy di dominio dove possibile, e nell'installazione di default sia di office che di libreoffice	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
8	7	1	DIFESE CONTRO I MALWARE	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Min.	MS Outlook non è il client di posta standard utilizzato in azienda quindi non è definibile una policy di dominio. In fase di installazione del client la funzionalità viene comunque disabilitata.	2017
8	7	4	DIFESE CONTRO I MALWARE	Disattivare l'anteprima automatica dei contenuti dei file.	Min.	Le funzionalità di anteprima automatica sono disattivate da policy locali sull'immagine dei client attualmente in distribuzione. Analogamente le funzionalità sono disabilitate anche tramite policy di dominio.	2017
8	8	1	DIFESE CONTRO I MALWARE	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione	Min.	La policy di Sophos configurata come standard per i client e per i server prevede la scansione dei supporti rimovibili al momento della loro connessione per Virus, Adware e PUA.	2017
8	9	1	DIFESE CONTRO I MALWARE	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Min.	La posta in ingresso della ASST è sottoposta a controllo antispam e antivirus tramite un apparato dotato di Sophos E-mail Appliance. In caso di segnalazione di spam il messaggio viene cancellato direttamente. Per allegati sospetti e spam con bassa reputazione il messaggio viene depositato in un'area di quarantena. I messaggi in quarantena vengono sottoposti ad analisi ad ogni rilascio di aggiornamenti ed eventualmente rilasciati o cancellati.	2017
8	9	2	DIFESE CONTRO I MALWARE	Filtrare il contenuto del traffico web.	Min.	Il filtraggio del traffico web è gestito dal sistema di proxy interno basato sia su liste pubbliche sia su liste che vengono personalizzate in base alle esigenze aziendali. Quindi per es. sono bloccati tutti gli accessi ai social network ma vengono resi disponibili siti quali YouTube utilizzati a fini didattici.	2017

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
8	9	1	DIFESE CONTRO I MALWARE	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).	Min.	sia il sistema di proxy che il sistema di antispam bloccano la tipologia degli allegati considerata pericolosa o non ideonea	2017
8	10	1	DIFESE CONTRO I MALWARE	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Std.	L'antivirus è in grado di rilevare le minacce non solo basandosi sul database delle firme integrato, ma anche tramite analisi del comportamento sospetto (HIPS) e rilevamento di traffico malevolo. Inoltre è in grado di rilevare e bloccare malware di classe crypto-ransomware analizzando il comportamento sospetto e richieste di connessione a server di generazione della chiave crittografica. I client sono costantemente connessi alla console centralizzata e scaricano i database delle firme aggiornati appena disponibili nell'infrastruttura locale, oltre a riportare alla console centralizzata eventuali minacce rilevate e comportamenti sospetti	2019
8	11	1	DIFESE CONTRO I MALWARE	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.	Std.	E' previsto nella piattaforma di trouble ticketing il tipo di incident "Sicurezza". Oltre questo in situazioni sospette viene effettuato il submit del sample file a Sophos per ulteriori analisi.	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
10	1	1	COPIE DI SICUREZZA	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Min.	Le informazioni per il ripristino dei sistemi perimetrali, di firewall e proxy vengono salvate dopo tutte le modifiche, anche più volte al giorno. Così anche tutte le informazioni relative a storage, sistema di backup, switch e telefonia. Tali copie vengono eseguite su supporto messo in sicurezza (esterno al sistema). È in fase di implementazione una procedura per l'organizzazione dei salvataggi con i sistemi attuali. È in fase di valutazione l'esigenza di un software per i salvataggi automatici.	2017
10	1	2	COPIE DI SICUREZZA	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.	Alto	Il documento di qualità SIA MO-030 è la nostra attuale procedura di backup. I sistemi di Ingegneria Clinica contrattualizzati o in via di contrattualizzazione prevedono l'incarico al fornitore di configurazione dei back up e ripristino di sistemi entro determinati SLA operativi. Per i sistemi virtualizzati il ripristino della macchina è in carico al SIA mentre per i sistemi fisici è a carico di ciascun fornitore (salvo per le macchine acquistate dal SIA) come nel caso del sistema RIS-PACS. Le contrattualizzazioni tendono ad uniformare la politica di back up e restore dei sistemi. In particolare vengono contrattualizzate le operazioni di manutenzione ordinaria che prevedono tra l'altro la verifica delle corrette operazioni di back up e le verifiche di congruità dei rispettivi DB.	2018
10	1	3	COPIE DI SICUREZZA	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore	Alto	Il documento SIA MO-030 spiega le diverse procedure e tipi di backup aziendali programmati	2018
10	7	1	COPIE DI SICUREZZA	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Std.	I test di ripristino vengono fatti all'installazione e poi in ambiente di test	2018

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
10	3	1	COPIE DI SICUREZZA	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.	Min.	Nel documento di qualità SIA-MO-030 è spiegato come i dati archiviati in cloud (quindi backup di secondo livello) vengono copiati dopo essere stati cifrati all'origine.	2018
10	6	1	COPIE DI SICUREZZA	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	Min.	Per la parte dati (data office, db, immagini, ecc.), la copia di archiviazione viene spostata sulla soluzione di archiviazione cloud aziendale la cui sicurezza è garantita dal fornitore. I dati così archiviati vengono cifrati all'origine	2017
13	1	1	PROTEZIONE DEI DATI	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	Min.	è in corso di acquisizione la soluzione dlp proposta in consip. Questa soluzione permetterà l'analisi dei dati esistenti e individuerà quelli ai quali andrà applicata la protezione crittografica	2018
13	2	1	PROTEZIONE DEI DATI	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Std.	la cifratura per i dispositivi portatili che contengono informazioni rilevanti o dati sensibili fa parte del progetto che si sta avviando con l'acquisizione del sistema dlp	2018
13	3	1	PROTEZIONE DEI DATI	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.	Alta	sono implementati firewall per il blocco del traffico non autorizzato e sistemi di navigazione per il content filtering. A questo sistema già esistente verrà affiancato un sistema dlp (in fase di acquisizione)	2019
13	4	1	PROTEZIONE DEI DATI	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.	Alta	il sistema dlp che si sta acquisendo permette di impostare in maniera automatica delle scansioni configurate per le necessità dell'azienda	2019
13	5	1	PROTEZIONE DEI DATI	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.	Alta	il sistema dlp che si sta acquisendo permette di impostare il blocco della scrittura di dati su supporti esterni	2019

1°	2°	3°	Classe	Descrizione Misura		Modalità di implementazione	Tempistiche
13	5	2	PROTEZIONE DEI DATI	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.	Alto	è già stato affidato all'attuale gestore dell'infrastruttura lo studio di un progetto per bloccare dispositivi non autorizzati e per gestire quelli autorizzati utilizzando delle liste aggiornate	2019
13	6	1	PROTEZIONE DEI DATI	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.	Alto	è in corso di acquisizione la soluzione dlp proposta in consip che potrà monitorare e controllare i flussi di dati	2019
13	6	2	PROTEZIONE DEI DATI	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Alto	sia i firewall che i proxy registrano il traffico e permettono l'analisi off line	2019
13	7	1	PROTEZIONE DEI DATI	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Alto	è in corso di acquisizione la soluzione proxy proposta in consip. Il traffico verrà monitorato rilevando le connessioni con crittografia	2019
13	8	1	PROTEZIONE DEI DATI	Bloccare il traffico da e verso url presenti in una blacklist.	Min.	il proxy interno gestisce sia whitelist che blacklist. È quindi possibile, in base alle varie categorizzazioni, bloccare l'accesso a server di file sharing oppure abilitare l'accesso a db con informazioni scientifiche e mediche per permettere studi approfonditi	2017
13	9	1	PROTEZIONE DEI DATI	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	Alto	il sistema dlp che si sta acquisendo permette di limitare la copia e implementa le regole di accesso impostate sui dati residenti sui server in dominio	2019

Generale:

Documento PKCS#7:	
Status documento:	Firmato digitalmente
Nome file p7m:	C:\Users\alati-99060 \AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\8MN0EOJ0 \ASST Monza - Misure Minime di Sicurezza AgID-27122017 pdf (3).p7m
Impronta SHA1 (hex):	39 B8 EF 77 9B 5D 4A 23 3A 18 4C 13 5B 1D 2E FC DB 43 B7 08
Impronta SHA256 (hex):	F5 60 66 E8 2B 51 64 6D 5C 8A B4 8C 7A 69 61 F1 06 70 A0 F1 26 01 96 30 5B B9 5E CC 53 05 F5 75
Contenuto:	
Tipo documento:	Documento PDF
Nome file originale:	ASST Monza - Misure Minime di Sicurezza AgID-27122017.pdf
Dimensioni:	171 KB (175532 bytes)
Impronta SHA1 (hex):	53 FB 4B 30 C9 EE 65 EE 6A 94 0C 2C 87 53 CF 0F 47 60 9E E6
Impronta SHA256 (hex):	25 14 93 43 0D 07 FC 9E 98 9D DD 9C DD 87 E8 39 94 35 ED AE EE FF D8 09 9F 43 DD 0D 0C BC D7 6B

Firme digitali CAdES (2):

MATTEO STOCCO

Sottoscrizione MATTEO STOCCO	
Risultato verifica:	
Stato della firma:	Valido
Stato del certificato:	[04/04/2018 15:13:57] - Valido, CA Accreditata, non sospeso o revocato.
Condizioni di verifica:	**VERIFICA CRL OFFLINE**
Certificato:	
Algoritmo certificato:	sha256WithRSAEncryption
S.N. certificato:	0096 66
Valido dal:	martedì 28 maggio 2013 14:19:09
Valido sino al:	lunedì 28 maggio 2018 14:19:09
Soggetto:	
Nome:	MATTEO
Cognome:	STOCCO
Codice fiscale:	STCMTT68H04F205X
Data di nascita:	<non disponibile>
Ruolo:	<non disponibile>
Paese:	IT
Certificato emesso da:	

Nome:	Servizio di Certificazione per la Firma Digitale - CA2, Lombardia Informatica S.p.A., IT
Paese:	IT
Firma documento:	
Algoritmo di firma:	RSA-sha256 (1024)
Firma digitale (hex):	19D7 10A9 91C4 734B B711 FECF 46CA B141 8C72 56E7 CA75 5955 8641 C2EA B0D4 6146 6CC7 2DB8 3CCF 5D31 A38E 3F03 D9D2 E1E3 87F7 4A58 4689 9FD1 8666 8FDB 0FA0 F38A 8B44 D78C 69B8 A812 E3BA 33CD 8BED 5EF0 4963 7ED6 A5D1 E74D 5716 E3B8 5F4C AE55 536E 45C3 9C9C F109 B4AE 033B A5BA 7AA4 24E3 081F 7C06 CC51 913F ED68 1B04 64B8
Attributi 'signed':	
contentType	pkcs7-data
signingTime	29/12/2017 10:38:48 GMT
messageDigest	25 14 93 43 0D 07 FC 9E 98 9D DD 9C DD 87 E8 39 94 35 ED AE EE FF D8 09 9F 43 DD 0D 0C BC D7 6B
id-aa-signingCertificateV2	sha256(D9 A4 FC 6E C4 8B BE 64 48 DA 01 0C 7F 60 BD EF C5 1B 31 B3 25 4C 86 3D F8 75 30 04 27 53 C1 A5) issuer(Servizio di Certificazione per la Firma Digitale - CA2, Lombardia Informatica S.p.A., IT) serial(009666)
Attributi 'unsigned':	
unstructuredName	PKCS7-File-HeaderDescription=;Filename=ASST Monza - Misure Minime di Sicurezza AgID-27122017.pdf;

ANDREA AMATO

Sottoscrizione ANDREA AMATO	
Risultato verifica:	
Stato della firma:	Valido
Stato del certificato:	[04/04/2018 15:13:57] - Valido, CA Accreditata, non sospeso o revocato.
Condizioni di verifica:	**VERIFICA CRL OFFLINE**
Certificato:	
Algoritmo certificato:	sha256WithRSAEncryption
S.N. certificato:	01AC 80
Valido dal:	mercoledì 7 dicembre 2016 16:23:56
Valido sino al:	sabato 7 dicembre 2019 16:23:56
Soggetto:	
Nome:	ANDREA
Cognome:	AMATO
Codice fiscale:	MTANDR57T22F704R

Data di nascita:	<non disponibile>
Ruolo:	<non disponibile>
Paese:	IT
Certificato emesso da:	
Nome:	Servizio di Certificazione per la Firma Digitale - CA2, Lombardia Informatica S.p.A., IT
Paese:	IT
Firma documento:	
Algoritmo di firma:	RSA-sha256 (2048)
Firma digitale (hex):	4A98 BA6A 4F49 396B D570 7D95 ADC8 C5DE E04E 51EC AFBF 641F 3F22 AF8A 6F3A 4A4E 1FAA AC99 304F 2587 46CB C3BB BC9F A419 C8CF AF1E BCC6 7217 6E21 10F1 1880 092A BE38 3ACD 5EEC 4B99 328F 2743 2FF1 19E7 03C2 635F 1F1F 3516 C9ED 8202 3837 0CEE 1ABF A4B5 EF67 7A75 4614 562E A5D8 85EB FC12 B34F 2FE1 1DED 5945 981B 29C1 11EB 8A9B BD86 8077 6341 85CA 2AC4 01FD 3048 0553 0C1F 976D C48B C59B B567 7FBE 5989 0063 2723 4788 977B E76C 72F9 2481 7CAB 86B5 EC06 9F43 A87A CB4E 5E5A 57DB E1BF 9768 B4D9 161F 78F1 98FE 0510 E84C 81EC A27B 184E 1564 177E FF93 3DB0 C759 F011 9EF2 E304 3095 2240 8C88 0459 09C3 F3C6 861F 8118 D2AA 1935 D52F AF97 00DE F7F5
Attributi 'signed':	
contentType	pkcs7-data
signingTime	27/12/2017 16:48:18 GMT
messageDigest	25 14 93 43 0D 07 FC 9E 98 9D DD 9C DD 87 E8 39 94 35 ED AE EE FF D8 09 9F 43 DD 0D 0C BC D7 6B
id-aa-signingCertificateV2	sha256(DC 29 1A A0 EF 63 CA 72 C7 07 37 33 A9 B4 2F 9A B4 DA 97 AF DC 49 98 12 39 8B 73 F7 F8 D7 4E 53) issuer(Servizio di Certificazione per la Firma Digitale - CA2, Lombardia Informatica S.p.A., IT) serial(01AC 80)
Attributi 'unsigned':	
unstructuredName	PKCS7-File-HeaderDescription=;Filename=ASST Monza - Misure Minime di Sicurezza AgID-27122017.pdf;

Certificati (2):

MATTEO STOCCO

Stato del certificato:	[04/04/2018 15:13:57] - Valido, CA Accreditata
Condizioni di verifica:	DB autenticato da DigitPA

Algoritmo certificato:	RSA-SHA256
S.N. certificato:	009666
Valido dal:	martedì 28 maggio 2013 14:19:09
Valido sino al:	lunedì 28 maggio 2018 14:19:09
Soggetto:	MATTEO STOCCO
Certificato emesso da:	Servizio di Certificazione per la Firma Digitale - CA2, Lombardia Informatica S.p.A., IT
Paese:	IT

ANDREA AMATO

Stato del certificato:	[04/04/2018 15:13:57] - Valido, CA Accreditata
Condizioni di verifica:	DB autenticato da DigitPA
Algoritmo certificato:	RSA-SHA256
S.N. certificato:	01AC80
Valido dal:	mercoledì 7 dicembre 2016 16:23:56
Valido sino al:	sabato 7 dicembre 2019 16:23:56
Soggetto:	ANDREA AMATO
Certificato emesso da:	Servizio di Certificazione per la Firma Digitale - CA2, Lombardia Informatica S.p.A., IT
Paese:	IT