COMUNE DI
REGGIO NELL'EMILIA

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA

(Circolare AGID 18/04/2017 n. 2)

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario patrimoniale dei beni informatici viene mantenuto aggiornato attraverso l'incarico ad una ditta esterna che a provvede ad etichettare i dispositivi acquisiti prima che vengano inseriti in rete. Dal punto di vista tecnico tutti i pc, portatili e telefoni VOIP collegati in rete sono gestiti dal DHCP. Quindi accedendo ad uno dei due server attivi è possibile verificare quali sono i dispositivi in esso registrati. Per tutti i dispositivi che non possono/devono gestire l'attribuzione automatica dell'indirizzo IP dal DHCP (es: stampanti di rete, server, apparati di rete, postazioni particolari, telecamere, ecc.) viene gestito, tramite un applicativo sviluppato internamente (Gestione Risorse Ced), l'elenco delle risorse di rete attive. Per ogni oggetto viene riportato almeno l'indirizzo IP, il nome, la descrizione, il tipo e la categoria. L'archivio è aggiornato ogni volta che viene aggiunto/modificato un elemento in rete ed è gestita l'ultima data di modifica. Inoltre tutte le PdL (sia desktop che portatili) e i server windows sono inventariate automaticamente all'interno della piattaforma Microsoft System Center Configuration Manager. Al momento l'ente non ha reti wireless che permettano l'accesso alla propria rete a dispositivi mobili. Inoltre è in corso di attivazione un sistema di Network Access Control per monitorare ed autorizzare i dispositivi che richiedono l'accesso in rete. Questo sistema utilizzando lo standard 802.1x, un proxy radius e repository interni consentirà l'ingresso in rete ai soli dispositivi "autorizzati" e previa verifica che le credenziali fornite siano valide nel dominio Active Directory. I dispositivi "autorizzati" sono quelli registrati nel dominio o nel repository del sistema NAC ed identificati tramite il Mac address o l'identificativo OUI.

					Le rete wireless per l'accesso alla risorse interne sarà disponibile solo contestualmente all'attivazione del NAC che ha tra i requisiti l'applicazione delle stesse regole di accesso per la rete wired anche alla rete wireless
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	E' attivo il software Microsoft System Center Configuration Manager per monitorare e gestire tutte le PdL e i server Windows.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	E' in corso di attivazione un sistema di Network Access Control per monitorare ed autorizzare i dispositivi che richiedono l'accesso in rete. Questo sistema utilizzando lo standard 802.1x, un proxy radius e repository interni consentirà l'ingresso in rete ai soli dispositivi "autorizzati" e previa verifica che le credenziali fornite siano valide nel dominio Active Directory. I dispositivi "autorizzati" sono quelli registrati nel dominio o nel repository del sistema NAC ed identificati tramite il Mac address o l'identificativo OUI.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	-
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	-
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	-
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Le direttive interne al Servizio impongono al personale che effettua interventi tecnici sugli apparati di reti/cablaggi postazioni pc ecc. di non lasciare prese di rete attive e non utilizzate. Inoltre nel regolamento comunale è fatto divieto ai dipendenti di utilizzare / collegare alla rete dispositivi non autorizzati. Vedi ABSC 1.1.1
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	E' attivo il software Microsoft SCCM per monitorare e gestire tutte le PdL e i server Windows.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Vedi ABSC 1.1.1
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o	-

				personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	-
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	E' in corso di attivazione un sistema di Network Access Control per monitorare ed autorizzare i dispositivi che richiedono l'accesso in rete. Questo sistema utilizzando lo standard 802.1x, un proxy radius e repository interni consentirà l'ingresso in rete ai soli dispositivi "autorizzati" e previa verifica che le credenziali fornite siano valide nel dominio Active Directory. I dispositivi "autorizzati" sono quelli registrati nel dominio o nel repository del sistema NAC ed identificati tramite il Mac address o l'identificativo OUI.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	-

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Le direttive del Servizio Informatica e il regolamento del personale vietano l'installazione di software non autorizzato sulle postazioni di lavoro. Tutte le postazioni sono configurate e sono attive policies di dominio per impedire l'installazione di software da parte dell'utente. L'utente non è amministratore del proprio pc e non ha diritti di accesso a cartelle /porzioni di registro generalmente utilizzate durante l'installazione di software. L'installazione di software sui server è effettuata ESCLUSIVAMENTE da parte del personale tecnico del Servizio Gestione e Sviluppo delle Tecnologie previa autorizzazione del dirigente o di un suo incaricato. Le postazioni PC sono installate con un'immagine standard che contiene un insieme di software utilizzato in tutto l'ente (es: Libreoffice, Google Chrome, VLC Media player, Aruba Sign, ecc.) a cui si aggiungono applicazioni specifiche installate sempre dal personale tecnico del Servizio Gestione e Sviluppo delle Tecnologie previa autorizzazione del dirigente o di un suo incaricato Su tutti i sistemi Microsoft (sia desktop che portatili che server) è attivo l'agente di System Center Configuration Manager che consente di avere report in tempo reale dei software installati su ogni sistema e relative versioni. L'elenco dei software installati sui sistemi Linux è invece gestito manualmente all'interno dell'applicativo sviluppato internate Gestione Risorse Ced e viene aggiornato dai sistemisti abilitati a questo tipo di operazioni ad ogni modifica. All'interno dello stesso applicativo interno sono registrati comunque anche le piattaforme e relative versioni per i server windows. Per i server in gestione a software houses esterne nella liberatoria per l'accesso remoto viene indicato il software presente ed è riportata una clausola per cui l'ente dovrà autorizzare preventivamente qualsiasi software sia necessario aggiungere.

					Questa clausola verrà anche indicata anche nella nomina ad amministratori esterni nell'ambito delle attività per l'adeguamento al GDPR
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	Vedi ABSC 2.1.1
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	-
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	-
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Vedi ABSC 2.1.1
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Vedi ABSC 2.1.1
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Vedi ABSC 2.1.1
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	-

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutte le postazioni pc vengono create e gestite con un'immagine standard e con policies di dominio. L'immagine standard è stata creata con l'obiettivo di limitare le azioni degli utenti che possano compromettere la propria postazione o la rete dell'ente. L'utente pertanto non puo' installare software, modificare configurazioni (es impostazioni dei browser installati, associazione delle estensioni), creare/modificare utenti e gruppi locali, modificare i permessi su file system ecc. Per la gestione dei dispositivi mobili è in corso di definizione l'attivazione di un sistema di Mobile Deployment Management in modo da poter definire le app utilizzabili per l'accesso alle risorse, impostarne la configurazione e le relative politiche per la salvaguardia dei dati. I server windows vengono invece creati a partire da un template sull'infrastruttura vmware. Le modalità con cui è creato questo template e con cui viene periodicamente aggiornato sono descritte nel documento "MM_regole per la creazione template windows". Nella rete dell'ente sono presenti server Red Hat Enterprise Linux. La ISO utilizzata per installare questi server Linux contiene già un template che permette di installare varie tipologie di server linux: minimo, database, web server, ecc. Generalmente I server vengono installati con il template di tipo web server, cui sono poi aggiunti I pacchetti minimi che servono per nuovo server che si sta creando. Per i server legati al sistema di posta Zimbra in gestione ad una software house esterna la stessa garantisce che i sistemi in loro gestione vengono installati e mantenuti tramite procedure automatizzate che consentono di mantenere allineate tutte le macchine in loro manutenzione.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente:	Vedi 3.1.1

				eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	-
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi 3.1.1
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	In caso di compromissione di una postazione PC si provvede alla formattazione e alla ricreazione ex novo con le modalità suddette e alla reinstallazione dei software specifici. Eventuali dati salvati in locale (e non in rete come suggerito dalle direttive dell'ente) sulla postazione, saranno successivamente ripristinati da un back-up, se disponibile. In caso di compromissione di un server è fondamentale capire quando è avvenuta la compromissione e qual'è il livello di gravità/invasività. A tal scopo l'ente ha attivato un servizio di rilevamento e analisi degli incidenti informatici di Certego che deve evidenziare in tempo reale eventuali attacchi e/o intrusioni. Grazie a questo servizio, effettuato da un team di specialisti in sicurezza e basato sull'analisi degli allarmi raccolti da una sonda installata in rete, il lasso temporale tra la compromissione di un server e la conoscenza dell'evento è pertanto ridotto al minimo. Presumibilmente quindi si avrà ancora a disposizione un back-up effettuato prima della compromissione. In tal caso si provvede a ripristinare il server dall'ultimo back-up valido, che nel caso dell'infrastruttura virtuale corrisponde alla copia dell'intero server. Qualora il server abbia agganciato partizioni / dati non inclusi nel back-up suddetto (es: dischi raw) si provvederà al ripristino da fonti differenti. Qualora la data di compromissione non sia certa, e

					l'intrusione molto invasiva si provvede alla reinstallazione completa del server a partire dal template.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	-
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini dei pc non sono memorizzate offline ma vengono costruite con un processo che le rende altrettanto sicure. L'immagine finale è infatti costruita in modo dinamico partendo dall'iso del sistema operativo ed applicando una Task sequence gestita tramite System Center Configuration Manager e non modificabile dagli operatori addetti alla preparazione delle postazioni. All'immagine standard si aggiungono dinamicamente policies di dominio modificabili solo dagli amministratori del domio stesso. Per i server Windows i template sull'ambiente virtuale sono conservate spente e quindi offline. Per i server Linux si parte sempre dell'immagine ISO che per sua natura è immodificabile.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Vedi 3.3.1. L'accesso alla piattaforma System Center Configuration Manager e a quella vmware in cui sono memorizzati i template è consentito solo agli amministratori di sistema
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte operazioni di amministrazione remota vengono fatte utilizzando protocolli sicuri: ad esempio SSH per i server Linux ed apparati di rete, Https per storage/appliance/ambiente virtuale, RDP per i server windows . In altri casi (es: Firewall) occorre avere una console software apposita installata sul pc e l'accesso al server di gestione è consentito solo ai pc nei locali del servizio gestione e sviluppo delle tecnologie. Qualora sia necessario utilizzare un protocollo non criptato l'accesso è consentito solo ai pc nei locali del servizio gestione e sviluppo delle tecnologie. L'accesso riservato alle postazioni "autorizzate" del servizio gestione e sviluppo delle tecnologie sarà ulteriormente rafforzato con l'introduzione del sistema NAC in corso di deployment. L'accesso amministrativo dall'esterno della rete dell'ente è consentito solo tramite accesso VPN SSL e previa sottoscrizione di apposita liberatoria ed installazione di certificato personale
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per	-

				assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	-
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	-
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	-
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	-
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	-

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	L'ente ha effettuato scansioni di vulnerabilità con cadenza annuale affidando l'incarico a ditte esterne che hanno utilizzato per la loro attività strumenti aggiornati . Attualmente l'ente ha attivato un servizio per il rilevamento, analisi e la risposta agli incidenti di sicurezza informatica basato su sonda Certego Panoptikon, come previsto dalla convenzione IntercentER della Regione Emilia Romagna "*servizi convergenti ed integrati di trasmissione dati e voce su reti fisse e mobili".* Il servizio suddetto prevede anche una sezione di rilevamento delle vulnerabilità accessibile tramite una dashboard consultabile dagli amministratori di sistema dell'ente. Il servizio include inoltre il supporto degli specialisti di Certego per le strategie di chiusura / limitazione dei rischi in base alle vulnerabilità evidenziate. La scansione delle vulnerabilità viene pertanto effettuata in tempo reale tramite un appliance inclusa nel servizio stesso ed in gestione ai tecnici di Certego. Sono inoltre in corso di valutazione uno dei seguenti strumenti aggiuntivi: • Accordo quadro con Dipartimento Ingegneria Informatica dell'università di Modena e Reggio o di Bologna per effettuare con cadenza definita (es: mensile) o a richiesta verifiche di vulnerabilità sui sistemi esposti su internet e fornire all'ente un report delle vulnerabilità riscontrate • Attivazione del servizio aggiuntivo di Certego dedicato esclusivamente alla ricerca delle vulnerabilità su tutti i sistemi server all'interno della rete
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Vedi 4.1.1

4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	-
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	-
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	-
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	-
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	-
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	-
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il servizio utilizzato per le scansioni di vulnerabilità è effettuato tramite una sonda installata in rete e gestito da una ditta specializzata in sicurezza ICT. L'aggiornamento dello strumento è pertanto garantito essendo fondamentale per assicurare l'efficienza del loro servizio
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Il servizio Certego di cui al punto 4.1.1 comprende anche una parte di consulenza che riguarda anche informazioni su nuove minacce e vulnerabilità e modalità di remediation.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Per i sistemi server Windows si utilizza WSUS che è stato configurato in modo da inviare automaticamente segnalazione sulla disponibilità di fix di sicurezza per i sistemi operativi e moduli Microsoft utilizzati. L'elenco delle Fix viene di conseguenza esaminato per identificare quelle attinenti: questo sono poi "autorizzate" per l'installazione su un insieme di server generalmente di test rappresentativi dell'ambiente di produzione.

					Dopo una settimana se non si riscontrano problemi particolari la distribuzione viene effettuata su tutti i sistemi. Il procedimento è analogo per le postazioni client e viene effettuato con System Center Configuration Manager con cadenza settimanale e su un sottoinsieme rappresentativo di postazioni (150 postazioni composto da 2 postazioni per ogni servizio). l'immagine standard viene aggiornata ogni 6 mesi per velocizzare il deploy della stessa. Ogni nuovo pc che viene preparato riceve automaticamente da System Center Configuration Manager tutti gli aggiornamenti sia del sistema operativo che applicativi distribuiti dopo l'ultimo versioning dell'immagine. Gli aggiornamenti del sistema operativo dei server Red Hat Enterprise Linux sono fatti settimanalmente tramite un comando che ricerca un eventuale aggiornamento e lo installa. Come per i server Windows sono aggiornate non solo il sistema operativo , ma anche, se installate, le componenti aggiuntive (es: JVM, Machine, Apache, Tomcat, Jboss). Anche in questo caso l'aggiornamento viene fatto sui server di test e, dopo un periodo di verifica riportato sulla produzione. Casi particolari relativi generalmente ad appliance basate su distribuzioni Linux, sono descritte nel documento "MM_template+aggiornamenti_Server_Linux.doc". Per i server di posta gestiti da una software house esterna gli aggiornamenti del SO vengono applicati 1 volta al mese salvo criticità di sicurezza che impattino sui servizi erogati. Sono previsti riavvi completi del sistema solo in caso di criticità relative al kernel. Gli aggiornamenti applicativi della suite Zimbra+Zextras sono fatti con cadenza almeno semestrale salvo criticità di sicurezza. Per quanto riguarda gli aggiornamenti applicativi occorre distinguere gli applicativi standard (es: acrobat, JVM, Plugin vari, strumenti per la produttività individuale, browser, ecc.) da applicativi specifici di gestione dell'attività dell'ente. Gli applicativi standard possono essere inclusi nell'immagine delle postazioni client o installati successivamente. Per gli applicativi standard che hanno un numero di installazioni generalmente superiore a 5 e

					che non presentano vincoli tecnologici tali da impedirne la distribuzione in modalità unattended, si utilizza System Center Configuration Manager sia per la prima installazione che per l'aggiornamento. Questo garantisce l'uniformità di versioni e di configurazione su tutto il parco client. L'aggiornamento di questi applicativi viene effettuato generalmente entro qualche mese dall'uscita della release compatibilmente con verifiche di compatibilità con eventuali applicativi specifici che lo utilizzano e conformità con il licenziamento attivo (in caso di software non open source). L'iter di aggiornamento è il seguente: - attivazione della nuova versione in laboratorio presso il servizio informatica: test di compatibilità da parte dei referenti applicativi che hanno in gestione software che lo utilizzano. Definizione di un tempo entro cui devono essere effettuati i test in relazione all'invasività del software da aggiornare - distribuzione automatica tramite System Control Configuration Manager ad un campione rappresentativo di postazioni. Definizione data di scadenza per i test - distribuzione automatica su tutte le postazioni Per quanto riguarda l'aggiornamento dei software specifici di gestione dell'attività dell'ente questi vengono installati prima in ambiente di test e poi in produzione dai sistemisti del Servizio Gestione e sviluppo delle Tecnologie dopo il rilascio da parte della software house e compatibilmente con le necessità organizzative degli uffici utilizzatori. In generale, per i sistemi in gestione a software house sono state date direttive per agire in modo conforme alle regole dell'ente. Durante le attività di adeguamento al GDPR queste direttive verranno formalizzate nella nomina ad Amministratori di sistema esterni.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Per i portatili, le direttive del servizio Gestione e sviluppo delle tecnologie e dei servizi informativi agli uffici impone il collegamento alla rete almeno ogni 15 giorni. In questo modo si garantisce che ricevano dai sistemi centrale gli aggiornamenti

					predisposti per tutte le postazioni client. Qualora ciò non venga fatto l'antivirus installato e non removibile dall'utente inibisce l'accesso in rete. Altri sistemi critici paragonabili a postazioni air-gapped sono quelle relative alla rete di videosorveglianza. L'aggiornamento di questi sistemi rientra contrattualmente nell'attività di manutenzione prevista dalla ditta fornitrice del sistema
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	-
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Nel documento "MM_vulnerabilità_v2" è riportato l'esito dell'ultimo test di vulnerabilità e le azioni messe in campo per la remediation necessaria. Tra le vulnerabilità evidenziate le più critiche sono quelle legate a sistemi operativi, sia client che server, dichiarati fuori supporto dal produttore e per cui non vengono più rilasciate patches di sicurezza. Si è pertanto provveduto a redigere un documento ("MM_sistemi_critici") in cui sono elencati i sistemi in questo stato, le applicazioni ad esso collegate, le motivazioni per cui il sistema deve essere mantenuto attivo, la descrizione dei rischi , le azioni necessarie alla chiusura/riduzione della vulnerabilità, gli incaricati, le tempistiche in cui si intende operare. Il documento di cui sopra è tenuto aggiornato a carico del responsabile della UOC Gestione delle Strutture Tecnologiche (Bondavalli Patrizia) per quanto riguarda l'elenco dei sistemi e dei rischi e dal responsabile della UOC Gestione dei Sistemi informativi (Leoni Barbara) per le rimanenti parti. Nel documento sono riportati anche eventuali sistemi su cui sono installati software middleware (es: tomcat, php, jboss, java, ecc) che non possono essere aggiornati per vincoli posti dalla software house che ha sviluppato l'applicativo che, in caso di aggiornamento, non ne garantirebbe il corretto funzionamento.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni	-

				sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Vedi 4.7.1
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Vedi 4.7.1
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	-
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Vedi 4.5.1 per l'aggiornamento dei software applicativi specifici dei servizi

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	L'accesso ai sistemi con privilegi amministrativi è consentito solo agli addetti del servizio gestione e sviluppo e tecnologie che hanno le competenze ed effettive necessità di modificare la configurazione dei sistemi. Come regola generale ci cerca di evitare di dare i privilegi amministrativi, ma eventualmente di dare l'accesso con ruolo "user" o di abilitare solo le funzioni necessarie (es: accesso a cartelle specifiche, possibilità di eseguire alcuni task, possibilità di riavviare alcuni servizi). Qualora la software house debba avere accessi amministrativi questi saranno limitati al sistema su cui è installata esclusivamente l'applicazione gestita dalla software house stessa. Gli utenti non hanno privilegi amministrativi sui pc.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Ogni persona fisica che deve effettuare accessi amministrativi ha due credenziali registrate su Active directory: una con diritti amministrativi e l'altra per l'attività ordinaria. E' stata data istruzione a tutti gli amministratori di sistema di utilizzare le credenziali amministrative solo per le operazioni per cui sono indispensabili. Ove tecnicamente possibile, sono stati abilitati o sono in corso di abilitazione i connettori verso AD in modo da utilizzare le credenziali corrette per l'accesso amministrativo. I log di accesso degli amministratori sono registrati su ogni sistema e, limitatamente ai sistemi che hanno dati personali, consolidati all'interno di neteye. Per quanto riguarda gli amministratori dei server di posta la software house interviene solo per attività che richiedono i privilegi amministrativi
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	-
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	-
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative,	Le utenze amministrative con particolare riferimento a quelle non

				garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	nominative sono registrate nel documento “Admin Password.xls” accessibile ai soli amministratori di sistema e/o all’interno dell’applicazione Gestione Risorse CED. Gli amministratori di sistema sono stati nominati formalmente e nell’ambito delle attività previste dal GDPR tali nomine saranno aggiornate, con particolare riferimento agli amministratori di sistema esterni.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	-
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Prima di collegare alla rete un dispositivo le password di default degli utenti amministratori vengono sostituite con altre corrispondenti alle regole dell’ente: questo può essere fatto in modo automatico (es: procedura di distribuzione dell’immagine standard, creazione nuovo server da template) o manualmente.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	-
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	-
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	-
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	-
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	-
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Le credenziali amministrative sono composte da uno user name di minimo 6 caratteri e da una password di minimo 8 caratteri. La password deve essere di elevata complessità in quanto le policies di dominio rendono obbligatori almeno un carattere speciale, una lettera maiuscola e una cifra. Per i server di posta gli accessi sono nominativi e dotati di chiave crittografica pubblica/privata personale cifrate con passphrase personale e pertanto di tipo “strong autentication” .

5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Vedi 5.7.1: le utenze amministrative sono create nel dominio Active Directory e non si possono registrare se non rispettano la regola di complessità definita
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le utenze amministrative nominative hanno l'obbligo di cambiare password ogni 90 giorni e rispettano il requisito al punto 5.7.4. Entrambi i vincoli sono gestiti configurando opportunamente la policy di dominio. Per i server di posta l'accesso è basato su chiave crittografica pubblica/privata personale e non su password e quindi non è necessario gestire la scadenza della stessa. E' in corso di verifica la possibilità di gestire la scadenza del certificato
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Dal 10/1/2018 verrà modificata nel dominio la policy che regola il riutilizzo della stessa password portandola da 1 a 10. Vedi 5.7.3 per i server di posta
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	-
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	-
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	-
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	-
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Vedi 5.1.2
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze sono nominative e riconducibili alla singola persona. Possono far eccezione a questa regola utenze per attività particolari (es: accesso a LDAP per leggere attributi, partenza task schedulati, partenza servizi applicativi, ecc.). I privilegi di queste utenze non nominative vengono ridotti al minimo per quanto tecnicamente possibile. Fanno eccezione anche le utenze amministrative anonime previste al ABSC 5.10.3

5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	E' stata data istruzione agli amministratori di sistema di utilizzare le credenziali amministrative anonime solo in caso di emergenza o per eseguire servizi o attività pianificate che debbano avere questo tipo di privilegi per funzionare. In quest'ultimo caso è in corso di verifica la possibilità di configurarle in modo da poter essere usate solo per quello scopo e non per attività interattive o per connettersi ai server.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Ove tecnicamente possibile, sono stati abilitati o sono in corso di abilitazione i connettori verso AD in modo da utilizzare le credenziali di dominio corrette per l'accesso amministrativo.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono accessibili solo agli amministratori di dominio visto che sono configurate opportunamente le ACL sul file system. In caso di indisponibilità del file system ne è conservata una copia cartacea in busta sigillata in cassaforte.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Per l'accesso ai server di posta in cui si utilizzano certificati la software house garantisce che le chiavi private sono mantenute sulle postazioni su dischi cifrati con altro sistema indipendente

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutte le postazioni e sui server Windows è installato l'antivirus Symantec Endpoint protection con gestione centralizzata ad aggiornamenti automatici. La gestione centralizzata consente di definire policies che l'utente non puo' modificare. Sui server Linux red hat dal sito ufficiale di RedHat si evince che, se si seguono le buone norme di RH, l'antivirus non è necessario. E' comunque in corso di valutazione la possibilità di installare Clam come antivirus di terze parti.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Sulle PDL è installato il firewall personale di Windows. Tutti gli accessi aono comunque governati centralmente dalle policies firewall e IPS gestite ed aggiornate sul Firewall Checkpoint
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Il regolamento del personale vieta l'uso ed il collegamento in rete di dispositivi non autorizzati. E' in corso di attivazione un progetto che prevede, tramite l'attivazione dello standard 802.1x e dalla piattaforma NAC di Extreme Networks, l'accesso alla rete ai soli dispositivi registrati all'interno del dominio e/o autorizzati centralmente tramite il Mac address ed in possesso di credenziali valide.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' attivata una Group Policy Object sul dominio che disattiva su tutti i PC l'esecuzione automatica dei contenuti sui dispositivi removibili
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Su Libreoffice è in corso di impostazione la configurazione che prevede un messaggio di accettazione prima di eseguire qualsiasi macro. La stessa configurazione è stata attivata su Microsoft Office.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Per la posta si utilizza esclusivamente la webmail e non è attivo nessun client di posta. Questo previene i rischi legati all'apertura automatica di email che hanno link / allegati pericolosi. Inoltre e' in corso di attivazione un modulo del firewall (checkPoint SandBlast) per intercettare ed eliminare mail con allegati/ url nocivi
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'antivirus Symantec Endpoint Protection non supporta la scansione automatica di dispositivi removibili nel momento dell'inseri-

					mento perché considerata troppo penalizzante per le prestazioni. E' invece attiva la funzionalità di auto-protect nel momento in cui accedo (anche in lettura) ai file presenti sul device esterno
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Sono attive due appliance Symantec Messagging Gateway per tutta la posta in ingresso
8	9	2	M	Filtrare il contenuto del traffico web.	Sono stati attivati sul firewall Checkpoint da cui tutti i client/server devono passare per accedere ad internet moduli di application control e URL filtering
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Sono attive policies sulle appliance Antispam per rimuovere allegati potenzialmente pericolosi. Sul firewall sono attive regole per evitare il download di file con estensioni (es: exe, zip, jar, ecc.) che possono avere contenuti malevoli. E' in corso di attivazione Il prodotto CheckPoint SandBlast per il blocco di messaggi di posta con allegati che contengono malware o il download di file malevoli (es. ransomware)

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Le copie di sicurezza di tutti i sistemi server/database/posta vengono fatte giornalmente utilizzando EMC Legato Networker e gli strumenti nativi di Vmware (piattaforma di virtualizzazione utilizzata) su un sistema di deduplica hardware EMC DataDomain. Sono poi definite delle regole di replica giornaliere verso un sistema analogo nel datacenter di Lepida a Ravenna. Per alcuni sistemi critici (posta e DB oracle) vengono fatte copie parziali (es: transactional log, variazioni) più frequentemente rispetto alla cadenza giornaliera.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	-
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	-
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	-
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	I dispositivi su cui vengono effettuate tutte le copie di sicurezza si trovano in locali del servizio Gestione e sviluppo delle Tecnologie con accesso controllato tramite badge e consentito solo al personale del servizio stesso. Tali locali sono inoltre protetti da sistemi di videosorveglianza e antifurto. La stessa cosa vale per il datacenter di Lepida SPA a Ravenna su cui viene effettuata la seconda copia necessaria per il disaster recovery. Inoltre le copie vengono effettuate tramite software appositi (EMC Legato Networker) che le rendono inutilizzabili se accedute con altri strumenti. E' in corso di verifica la possibilità di attivare l'encryption all'interno del protocollo boost utilizzato per il backup.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I dispositivi su cui vengono fatte le copie sia presso l'ente che presso il datacenter di lepida SPA non sono direttamente accessibili come unità di rete sui sistemi contenenti i dati sorgente, poichè il backup viene effettuato tramite un software specifico (EMC Legato Networker) su dispositivi hardware di deduplica (EMC DataDo-

					main) ed il job di backup è attivo solo in momenti ben precisi identificati dalle policy impostate dall'ente

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). Nell'ambito degli adempimenti necessari per il GDPR verrà fatta un'analisi dei dati per verificare quali hanno particolari requisiti di riservatezza e sarà valutata la possibilità di dare ad ogni servizio dell'ente uno spazio di memorizzazione criptato all'interno del datacenter di lepida SPA.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	-
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	-
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	-
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	-
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	-
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	-
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	-
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che	-

				usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	E’ attivo il modulo URL filtering sul Firewall Checkpoint e le relative regole che bloccano l’accesso a siti appartenenti a categorie pericolose (es: hacking) e/o non attinenti all’attività lavorativa (es: gaming)
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

IL DIRIGENTE

IL RESPONSABILE LEGALE