ALLEGATO M: REQUISITI MINIMI DI SICUREZZA

Nello schema seguente sono state descritte le modalità di implementazione relativamente ai requisiti di livello M, ovvero quelli che rappresentano per lo più lo stato attuale dell'Azienda.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI: Sono stati analizzati solo i Requisiti Minimi

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Compliant Il blocco della connessione per i dispositivi non autorizzati è normato dal regolamento Aziendale Attualmente la ASL 3 dispone di inventari realizzati con sw differenti in base alle diverse categorie di dispositivi. Le postazioni di lavoro sono inventariate non automaticamente sulla piattaforma HP Service Manager che ne permette la gestione remota e il controllo delle postazioni e dei dispositivi (stampanti) connessi. Tale applicazione mantiene anche la correlazione tra pc/portatili e utenti ai quali sono assegnate le risorse. La console centralizzata dell'antivirus Symantec Endpoint Protection permette di visualizzare la lista di tutti i server e client con relativo indirizzo IP sulle quali tale sw è installato. L'inventario di tutti i sistemi server fisici e virtuali in gestione a Liguria Digitale	Aggiornare Il Regolamento Aziendale sull'utilizzo delle dotazioni informatiche per regolamentare oltre all' utilizzo dei dispositivi aziendali anche gli extraziendali eventuali e stabilendo le tipologie di dispositivi autorizzati esterni all'azienda (dispositivi connessi tramite VPN, dispositivi mobili connessi tramite wifi) Impedire l'accesso alla rete aziendale e VPN ai dispositivi che non sono inventariati e/o successivamente autorizzati. Attivare un servizio di autenticazione con utenza di Dominio che separi la rete per i dispositivi aziendali da quella per i dispositivi personali,

					viene mantenuto all'interno di un CMDB che contiene anche le informazioni di configurazione e del sw installato. L'inventario dei cellulari, smartphone e tablet aziendali è mantenuto in un elenco aggiornato manualmente: Esiste un inventario su foglio Excel degli apparati di rete installati e viene aggiornato manualmente. L'elenco degli elettromedicali attivi è contenuto all'interno di un censimento costantemente aggiornato in cui però non viene evidenziato la connessione in rete o stand-alone. Non è ammesso da Regolamento Aziendale sull'utilizzo delle dotazioni informatiche l'utilizzo in rete Aziendale l'utilizzo di dispositivi personali .	limitando questi ultimi alla sola navigazione Internet. Tracciare sul censimento delle apparecchiature elettromedicali l'eventuale collegamento in rete.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Compliant con le limitazioni di cui al punto 1.1.1 Il collegamento alla rete di ASL3 dei dispostivi autorizzati avviene dopo una procedura di inserimento manuale sulla piattaforma HP service Manager che ne garantisce la gestione centralizzata. L'inventario contenuto nel CMBD viene	Aggiornamento del preesistente regolamento relativo all'utilizzo delle attrezzature informatiche aziendali. Attivare un servizio di autenticazione con utenza di Dominio che separi la rete per i dispositivi aziendali da quella

					aggiornato ogni qual volta si connette un nuovo server alla rete. L'aggiornamento dei nuovi apparati di rete connessi avviene manualmente	per i dispositivi personali, limitando questi ultimi alla sola navigazione Internet. In tal modo associando i dispositivi autorizzati a ciascun utente di dominio viene regolamentato l'accesso di dispositivi alla intranet anche via wifi.
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.	Compliant Su un foglio di calcolo è tenuta traccia di tutti gli ip statici in uso e relative macchine . Tale corrispondenza è confermata dalla Console Antivirus e su HP Service Manager dove applicabile.	Verifica e aggiornamento inventario. Per i dispositivi BYOD, tablet e smartphone vedi ABSC_ID 1.1.1. e 1.3.1.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
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.	Compliant Esiste un elenco del software applicativi formalmente autorizzato. Le postazioni di lavoro sono configurate dagli amministratori di sistema e, poiché gli utenti non hanno diritti amministrativi, non è loro	Aggiornare l'elenco dei sw autorizzati ed inserirlo nel Regolamento Aziendale da aggiornare annualmente.

					consentito installare software in autonomia. Il CMDB mantiene un catalogo delle applicazioni implementate e del software installati sui sistemi server.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Compliant relativamente al contesto autorizzativo: Attualmente non vengono eseguite scansioni temporizzate per verificare il software installato in quanto, non essendo gli utenti amministratori non possono installare nulla sulle postazioni di lavoro(vedi Regolamenti Aziendale utilizzo dotazioni informatiche) Sui server sono installati solamente i software strettamente necessari al funzionamento dei relativi servizi.	E' comunque in fase di test il modulo symantec per la verifica dei sw autorizzati su macchine MS e Linux (server e client). Non appena validato può essere attivato.

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	Azioni migliorative
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Compliant Sia le postazioni di lavoro che i server vengono installati con configurazioni standard tali da garantire un livello di sicurezza adeguato, prevedendo ad esempio un numero minimo di porte di rete aperte e disponibili. Quando ritenuto necessario i sistemi vengono ulteriormente hardenizzati. Non è prevista una configurazione standard per quanto riguarda i dispositivi mobili.	Formalizzare e/o aggiornare la procedura di configurazione dei sistemi client e server. Pianificare la dismissione dei sistemi obsoleti che non permettono

						l'applicazione di configurazioni sicure (es. Windows XP).
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Compliant Esiste documento configurazioni standard	Ref. Action proposed ABSC 3.1.1 (Vedi Azione proposta ABSC 3.1.1.)
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Compliant I sistemi compromessi vengono ripristinati come da procedura a partire da immagini di backup integre.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Compliant Esistono copie offline delle immagini di installazione dei sistemi che possono essere utilizzate per effettuare verifiche di integrità.	Formalizzare in procedura la conservazione e manutenzione offline di immagini di installazione costantemente aggiornate ed implementare il livello S (3.3.2).
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Compliant Solo gli utenti autorizzati possono accedere alle immagini conservate su una macchina dedicata in rete con storage ridondato.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server,	Compliant /partially compliant per apparati di	Pianificare la

				workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	rete. Tutti i sistemi sono amministrati attraverso connessioni protette e ritenute sicure (SSH, RDP, HTTPS). Rimangono in uso alcuni apparati di rete obsoleti nei quali l'amministrazione remota tramite canali crittografati non è supportata E' in fase di predisposizione una configurazione di un sistema ACS (Access Contro System) su server Radius per la gestione degli apparati di rete	dismissione degli apparati obsoleti (che non supportano l'amministrazione remota tramite canali crittografati). Attivare il sistema ACS attualmente in fase di predisposizione.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
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.	Compliant sono a disposizione strumenti automatici gestiti da Liguria Digitale in grado di rilevare eventuali vulnerabilità su tutti i sistemi. Tali ricerche e relativi report sono eseguiti a seguito di segnalazione di nuove vulnerabilità o di significative modifiche della configurazione dei sistemi, su target critici in modo da non gravare significativamente sulle	Nell'ambito del contratto di Gestione in outsourcing con Liguria Digitale, definire procedure formali di scansione sistematica della rete per l'implementazione del livello Standard di cui al punto 4.1.2.

					prestazioni della rete.	
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.		
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Compliant Gli strumenti di scansione delle vulnerabilità sono aggiornati in modo automatico.	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Compliant Nei sistemi Microsoft, WSUS gestisce la verifica e l'installazione automatica degli aggiornamenti critici e delle patch di sicurezza del sistema operativo e delle applicazioni Microsoft. La gestione delle patch sui sistemi server è semiautomatica al fine di garantire la continuità dei servizi attivi. Attualmente non esiste una gestione centralizzata delle patch relative alle applicazioni non Microsoft. Al fine di garantire la continuità dei servizi in ambito ospedaliero, gli aggiornamenti che possono rivelarsi critici per applicazioni non interrompibili non sono installati automaticamente ma pianificati a seguito di esito positivo di test .	Valutare eventuale pianificazione di aggiornamenti sistematici centralizzati per sistemi Linux

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.	Non sono presenti sistemi isolati dalla rete poiché non ne sussistono le necessità	Verificare la presenza e necessità di sistemi air-gapped nella'rea elettromedicale
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.	Compliant Il personale adibito alla gestione della sicurezza di Liguria Digitale informa il personale IT delle principali vulnerabilità e minacce e, in accordo con esso, pianifica e verifica l'esecuzione delle relative contromisure. Il documento programmatico sulla sicurezza aggiornato contiene l'analisi dei rischi dei dati trattati dall'Ente.	Aggiornare periodicamente l'analisi dei rischi contenuta nel DPS.
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.).	Ad oggi non è disponibile un'analisi dei rischi relativi alla cyber security.	Inserire nel DPS l'analisi del rischi
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.	Compliant Per i sistemi client e server la procedura automatica prevede l'applicazione di tutte le patch relative ai rischi di sicurezza e di quelle ritenute critiche.	Prevedere aggiornamenti sistematici delle patch di sicurezza anche direttamente sugli apparati elettromedicali in rete.
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	Compliant Sulle applicazioni critiche le patch	

				nei sistemi in esercizio.	vengono preventivamente testate per valutarne gli impatti (4.5.1)	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
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.	Compliant Le utenze di amministrazione sono assegnate solo a personale idoneo e competente. Gli utenti non possiedono privilegi amministrativi nemmeno sulle macchine a loro assegnate	
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Partially Compliant Gli amministratori di sistema di Liguria Digitale utilizzano utenze amministrative sui sistemi di ASL3 unicamente per lo svolgimento di attività di gestione. Gli amministratori di sistema dipendenti di ASL3 possiedono utenze amministrative per lo svolgimento dell'intera attività lavorativa. I log degli accessi degli amministratori sono comunque raccolti da un sistema gestito da Liguria Digitale dai quali si	

					possono tracciare gli accessi	
5	1	3	S	Partially Compliant Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Partially Compliant A livello di server esistono privilegi differenziati per ciascuna utenza amministrativa. Per quanto riguarda i privilegi di amministratore dei client è possibile assegnare i privilegi di amministratore su diversi gruppi di macchine a gruppi di utenze di amministratore diverse.	Valutare l'impatto di definizione di policy più granulari su tutti i client.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Compliant L'inventario delle utenze amministrative è aggiornato ad ogni nuova assegnazione e formalmente autorizzata . Esiste lettera di incarico per gli amministratori di sistema di Liguria Digitale che specifica la responsabilità verso i sistemi client e verso gli amministratori di sistema dipendenti di ASL 3.	
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.	Compliant Prima di collegare alla rete un nuovo dispositivo le credenziali di amministratore predefinite vengono modificate secondo le policy delle password previste.	

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).	Compliant la lunghezza minima delle password degli amministratori attualmente non è impostata a 14 caratteri.	Formalizzare e impostare la lunghezza delle password di Amministratore a 14 caratteri con criteri di elevata robustezza. Verificare l'applicazione delle policy di robustezza delle password per i sistemi non gestiti centralmente.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Compliant Le policy MS impongono la modifica delle password almeno ogni 90 giorni, come prescritto dal Garante per la protezione dei dati personali.	Policy robustezza password vedi azioni proposte ABSC 5.7.1.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Compliant Le policy impediscono il riutilizzo delle ultime 4 password utilizzate.	Policy robustezza password vedi azioni proposte ABSC 5.7.1.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non compliant Non viene applicato il controllo temporale per problemi gestionali (password smarrite, reset..)	Applicare la policy temporale a tutti gli utenti tranne che per gli amministratori di dominio ai quali è concessa la modifica delle password degli utenti per ripristini, reser etc.
5	7	6	S	Assicurare che le stesse credenziali amministrative non	Partially compliant (cedi 5.7.6)	

				possano essere riutilizzate prima di sei mesi.	Non viene assicurato un tempo preciso ma viene impedito il restore delle ultime 3 password utilizzate	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Compliant Le utenze amministrative sono destinate esclusivamente ai gestori dei sistemi informativi e completamente distinte dalle utenze che non svolgono tali attività.	Vedi azioni proposte ABSC 5.1.2.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Compliant Sia le utenze standard che quelle amministrative sono personali . (All. B DLG 146/2003)	
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.	Compliant Di norma le utenze amministrative "root" e "Administrator" sono utilizzate solo in caso di emergenza.	Formalizzare la procedura per l'utilizzo di utenze amministrative anonime in caso di emergenza che comprenda la custodia delle password, la registrazione degli utilizzatori e la sostituzione della password.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Compliant Le credenziali amministrative sono conservate in busta chiusa accessibile ai soli amministratori di sistema in caso di necessità.	

5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Compliant Attualmente non è prevista l'autenticazione mediante l'utilizzo di certificati digitali. In caso di necessità è tuttavia a disposizione presso Liguria Digitale un sistema di gestione delle chiavi crittografiche.	Valutare l'implementazione di una Public Key Infrastructure (PKI) aziendale.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
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.	Compliant Tutti i sistemi gestiti centralmente e collegati alla rete locale sono dotati di sistemi antivirus la cui configurazione e aggiornamento è gestita in maniera centralizzata tramite la console di Symantec Endpoint Protection.	Inserire sempre nei requisiti di gestione degli elettromedicali la dotazione e la gestione degli antivirus analogamnete a quanto avviene per gli altri dispositivi informatici connessi in rete

8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Compliant I firewall locali sono attivi su sistemi di recente installazione nei quali tale protezione è attiva di default. Il software antivirus in uso è dotato di un modulo con funzionalità di IPS.	Verificare che antivirus e firewall locali siano attivi su tutti i sistemi.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Partially compliant Gli antivirus sono gestiti centralmente e monitorati per tutti i dispositivi in dominiio MS. Agli utenti, non essendo amministratori delle macchine , non è possibile altercarne la configurazione.	Monitorare la gestione degli antivirus anche su altri dispositivi (elettromedicali) per i quali non è possibile la gestione centralizzata
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Compliant Di norma l'utilizzo di dispositivi esterni non necessari per le attività lavorative è limitato. ed è normato dal Regolamento Aziendale	Aggiornare il "Documento programmatico sulla sicurezza" includendo una procedura per la verifica del rispetto della policy di utilizzo dei dispositivi esterni.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.		
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Compliant L'esecuzione automatica dei contenuti dei dispositivi removibili è disabilitata per tutti i sistemi Microsoft Windows client/server più recenti.	Aggiornare il Regolamento Aziendale definendo comunque norme di comportamento e policy per tutti gli utenti per la disattivazione dell'esecuzione automatica dei contenuti dinamici (unica cautela possibile per quei casi in cui non è possibile impedirlo

						tecnicamente).
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Compliant In tutti i sistemi Microsoft Windows client/server e nelle applicazioni più recenti è richiesta all'utente l'autorizzazione all'esecuzione di contenuti dinamici.	Vedi azioni proposte ABSC 8.7.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Compliant I client di posta in gestione a Liguria Digitale di norma impediscono l'apertura automatica dei messaggi come impostazione di default.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Not Compliant Al momento l'anteprima automatica dei contenuti dei file non è disabilitata poiché non ritenuta particolarmente significativa ai fini della sicurezza	Valutare l'impatto sugli utenti e le implicazioni di sicurezza di una policy che disattivi l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Partially Compliant La scansione avviene ad oggi prima dell'utilizzo della risorsa.	
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.	Compliant Requisito rispettato attraverso il servizio Antispam (Sophos) gestito da Liguria Digitale	
8	9	2	M	Filtrare il contenuto del traffico web.	Compliant Tutto il traffico web diASL 3 è filtrato da sistemi avanzati di content filtering (Fortinet)	

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).	Compliant Fare riferimento al gestore del servizio Antispam e Web Filtering (Sophos + Fortinet) gestito da Liguria Digitale	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Compliant I backup delle informazioni necessarie al ripristino dei sistemi server critici e dei sistemi virtuali sono schedulati settimanalmente (vedi allegato tecnico PTE Liguria Digitale e gestione sistemi LIS e PACS)	Inserire nel Regolamento Aziendale una policy che vieti di mantenere informazioni critiche sul disco locale non sottoposte ad attività di backup.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Partially compliant : Il ripristino di prova viene effettuato solo per immagini particolarmente critiche	Regolamentare il ripristino di prova per tutte le copie
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.	Compliant : I supporti fisici di conservazione dei backup sono adeguatamente protetti in locali chiusi accessibili al solo personale autorizzato e archiviati in cassaforte. Non viene effettuata attività di cifratura.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo	Compliant : I backup full di lungo periodo sono mantenuti offline su nastri magnetici.	

				possano coinvolgere anche tutte le sue copie di sicurezza.		

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
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	Partially compliant Non è prevista una attività sistematica di analisi e classificazione delle informazioni gestite dall'ente salvo nell'ambito di alcuni progetti. Un'analisi circa la riservatezza di diverse tipologie di dati è contenuta all'interno del DPS. Non vengono applicate protezioni crittografiche.	Analizzare la possibilità di applicazione di protezione crittografiche per le categorie più critiche; Raffinare l'analisi all'interno del DPS.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Compliant Tutto il traffico internet è filtrato da sistemi avanzati di content filtering in grado di bloccare i flussi da e verso URL non autorizzate (Fortinet).	