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 è conservato presso la direzione amministrativa del Conservatorio con accesso criptato. L'inventario elenca i dispositivi informatici collegati in rete in modo permanente ed è strutturato nel modo seguente: nominativo dell'apparato (inventario patrimoniale); • indirizzo IP statico • Collocazione • Eventuale assegnazione a persona specifica • Sistema Operativo Installato
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	L'inventario è implementato tramite excel
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	La scannerizzazione e il discovery degli indirizzi IP e del Mac è realizzabile mediante il software freeware Scan-to-All
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	N.N.
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Il DHCP è erogato dal router che registra tramite log le operazioni 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.	vengono monitorati i dispositivi collegati al segmento dell'amministrazione e a quello della didattica, che fanno accesso a reti distinte e separate.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento avviene all'atto dell'approvazione di un nuovo dispositivo e alla cessazione di dispositivi dismessi
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	N.N.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla	Si rimanda al punto 1.1.1.

				rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	
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.	Tutte le macchine operano tramite indirizzi IP assegnati dinamicamente dal server DHCP con registrazione dei log e adeguate politiche di lease time
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.	N.N.
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.	N.N.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	N.N.

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.	L'inventario è conservato presso la direzione amministrativa in apposito file criptato. L'inventario contiene: • tipologia dispositivo • nome del software • fornitore e/o marca • versione • soggetto autorizzante • eventuale data di scadenza dell'autorizzazione L'aggiornamento dell'elenco dei software è a carico dell'amministratore di sistema. Sono state date direttive al personale e di non installare alcun software diverso. In caso di necessità, questa viene evidenziata, e verificata la reale esigenza si provvede all'installazione e al censimento del nuovo applicativo. Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (vedi 5.1.1)
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.	Sarà implementato con l'adozione di un sistema di firewall hardware da acquisire nel breve periodo, al momento il controllo è manuale.
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	Non si ritiene al momento necessario.

				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.	Attuato tramite Win MD5 free - software free snello e di utilizzo immediato che utilizza la funzione hash crittografica MD5.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	il responsabile esegue ricognizioni periodiche per la verifica del software installato su ciascun dispositivo comparail risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco viene immediatamente disinstallato.
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.	Inventario di cui al punto 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.	Non sono necessari considerato che non vi sono elementi di rischio a ciò connessi. I dispositivi della segreteria sono monitorati direttamente dal responsabile della transizione digitale.
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.	Non sono presenti applicazioni che richiedono tali precauzioni.

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.	Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica. Per la rete dell'amministrazione si prevede oltre a quanto detto al punto precedente un antivirus per la navigazione in rete. Sono utilizzate copie immagine conservate come descritto al punto 3.3.1 e 3.3.2.
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: 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.	Per il segmento della didattica non si ritiene necessario attivare un sistema di controllo e configurazione specifica della strumentazione e si provvede, sulle macchine di proprietà dell'amministrazione: • alla rimozione di software non necessario • alla disabilitazione di servizi e moduli non necessari; Per il segmento dell'amministrazione si provvede: • rimozione di software non necessario dal sistema; • alla disabilitazione di servizi e moduli non necessari; • all'installazione di un firewall se compatibile con i software esistenti; • all'applicazione di permessi restrittivi sui file; • all'applicazione di policy per la complessità delle password; • rimozione degli utenti non necessari;
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	I sistemi operativi e i software utilizzati in Conservatorio sono di facile installazione e non richiedono procedure che non possano essere replicate in caso di crash.

				di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Si rimanda al punto 3.1.1.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sono vigenti disposizioni in tal senso.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	I cambiamenti sono autorizzati dal responsabile della transizione al digitale.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Non si ritiene necessario per la configurazione della rete e per il fatto che i principali software operano in modalità SAAP. I dati sono soggetti a backup su dispositivo NAS
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	N.N.
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).	Non è ancora attuata l'amministrazione remota dei computer presenti in amministrazione. Tutte le connessioni verso server esterni di importanza primaria avvengono attraverso canali sicuri (https, ftpd, ssh, ecc.)
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.	Il controllo avviene mediante il software antivirus, nonché software free (es. Malwarebytes Anti-Malware) per rilevare la presenza eventuale di malicious software (malware appunto).
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.	L'antivirus prevede l'alert automatico, visivo all'operatore, poiché è sempre attivo e ogni nuovo file eseguibile è scannerizzato in tempo reale.
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.	Non si ritiene necessario un livello di dettaglio in quanto è già sufficiente rilevare la minaccia e bloccare le successive operazioni.

3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Ogni operatore di segreteria monitora costantemente mediante il sistema antivirus ogni eventuale attacco esterno.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	N.N.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Le configurazioni sono standard e quindi non si ritiene necessario attivare ulteriori sistemi di ripristino rispetto a quelli previsti dal S.O. proprietario in uso (punti di ripristino a cadenza regolare).

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.	E' prevista l'utilizzazione del software SECPOD SANER. Il personale è informato della necessità di monitorare i sistemi e viene informato nel caso in cui gli organi di stampa e/o le autorità preposte segnalino particolari rischi.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Esiste la disposizione di effettuare una scansione almeno trimestrale delle vulnerabilità.
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).	Non è necessario dato il basso rischio e considerando che il punto in questione è orientato alla protezione di grandi organizzazioni.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non è necessario dato il basso rischio e considerando che il punto in questione è orientato alla protezione di grandi organizzazioni.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Non è necessario dato il basso rischio e considerando che il punto in questione è orientato alla protezione di grandi organizzazioni.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Non è necessario dato il basso rischio e considerando che il punto in questione è orientato alla protezione di grandi organizzazioni.
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.	Non è necessario dato il basso rischio e considerando che il punto in questione è orientato alla protezione di grandi organizzazioni.
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	Le scansioni vengono effettuate localmente dagli operatori.

				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.	Sono state date disposizioni agli operatori di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità
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	Non è necessario dato il basso rischio e considerando che il punto in questione è orientato alla protezione di grandi organizzazioni.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	È normalmente prevista sia dalla fase di installazione delle macchine. Vengono effettuati controlli per accertare la regolare installazione degli aggiornamenti.
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 esistono sistemi di tale categoria.
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.	In virtù del basso – medio rischio accertato non sono previste policy particolari.
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.	Sono state date disposizioni analoghe a quelle per il punto 4.4.1.
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.	Il responsabile della transizione al digitale accerta il livello di rischio, in contradditorio e in collaborazione con gli utenti.
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.).	E' in corso di redazione il DPP (Documento Programmatico in materia di Privacy) per la gestione del rischio informatico in generale. Si analizzano le azioni suggerite dal report prodotto dello

					strumento di scansione, agendo in base alle priorità ivi indicate.
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 4.8.1 e 4.5.1
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.	I dati sono in parte delocalizzati, invece, per quelli residenti in sede si eseguono regolari backup. Le patch pur necessarie non sono indispensabili per le attività quotidiane pertanto il presente punto non si ritiene applicabile.
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.	N.N.

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.	La rete associata al segmento della didattica è strutturata in modalità peer to peer ogni pc ha più account, i privilegi di amministrazione sono riservati ai soli responsabili (qualora i pc siano di proprietà dell'amministrazione). Nessuna disposizione per i dispositivi di terzi autorizzati all'accesso. Il segmento della didattica è separato da quello dell'amministrazione in modo fisico. La rete associata al segmento dell'amministrazione è di tipo peer to peer e ogni utente ha i privilegi di amministratore ciò si rende necessario per la gestione e il controllo completo dei software, degli aggiornamenti e delle minacce.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Non è necessario registrare gli accessi nella rete associata al segmento dell'amministrazione poiché vi è un rapporto 1:1 tra operatore e dispositivo. La rete associata al segmento della didattica non presenta tale necessità.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'architettura è peer to peer pertanto non esiste un server che permette la gestione dei privilegi; si aggiunge che per ora non se ne riscontra la necessità.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	N.N.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I documenti sono conservati dalla direzione amministrativa. È in corso la ricognizione precisa e puntuale al fine di giungere alla redazione di un inventario definitivo delle utenze.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	N.N.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le	Agli operatori sono state impartite adeguate istruzioni al riguardo.

				credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	N.N.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	N.N.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	N.N.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Non è necessario attivare protezioni poiché ogni pc dell'amministrazione è assegnato ad un solo operatore pertanto nessuno può accedervi. I pc sono localizzati in locali protetti e controllati fisicamente. Il problema non si pone per i pc del segmento della didattica.
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.	N.N.
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).	Sono fornite indicazioni a tutti gli utenti per l'utilizzo di password di autenticazioni "forti", "almeno 8 caratteri di cui uno speciale più un numero più una maiuscola"
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Vedi punto 5.7.1.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi. Misura che, in realtà, è già prevista obbligatoriamente dall'allegato B "Misure minime" del Codice Privacy
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Si sono date indicazioni di non riutilizzo delle ultime tre password.

5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Le misure di cui ai punti 5.7.3. e 5.7.4. sono sufficienti
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Le misure di cui ai punti 5.7.3. e 5.7.4. sono sufficienti
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.	Ogni pc ha almeno una doppia utenza. Il S.O. in uso non consente scambio dati in presenza di una sola utenza.
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.	Vedi 4.10.1.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Sono state impartite agli operatori disposizioni conformi a questa regola.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze del segmento amministrativo sono assegnate alla singola persona. Tale livello di protezione non è necessario nella rete del segmento della didattica.
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.	Sono state date indicazioni conformi alla regola qui descritta.
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).	Come specificato in premessa non è presente l'architettura client - server con la gestione dei domini e degli account.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Già previsto nella Privacy, vengono raccolte in busta chiusa e conservate dal responsabile del trattamento Le credenziali di accesso sono personali e quindi non possono essere conosciute

					e/o archiviate. Le credenziali non personali sono conservate in un file protetto da una password dal responsabile della transizione.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano certificati digitali per l'autenticazione delle utenze di amministrazione se non quelle di sistema.

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 tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico. Risulta inoltre presente software per il rilievo della presenza di malicious software con settaggio per l'aggiornamento automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC, portatili e altri dispositivi è attivato un firewall.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	N.N.
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.	N.N.
8	2	2	S	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.	N.N.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	N.N.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Nel disciplinare dei dipendenti è stata data disposizione di limitare l'uso di dispositivi esterni a quelli necessari per le attività di segreteria. Ciò non è possibile per la rete didattica che per sua natura non può essere limitata ma deve essere estesa anche ai dispositivi personali dei docenti e degli studenti. In caso di concerti, convegni, corsi e altri eventi con accessi di terzi possono essere create reti temporanee con accessi circoscritti nel tempo e nello spazio.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Non applicabile per le ragioni di cui al punto 8.3.1

8	4	1	S	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.	N.N.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	In alcuni casi è configurato e attivato microsoft windows defender.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Il software antivirus è ritenuto sufficiente
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	N.N.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Viene effettuato dal firewall personale.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi	Il conservatorio utilizza servizi di posta elettronica certificata e di

				raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	posta elettonica ordinaria acquisiti da ARUBA SpA che filtra le mail con un sistema antispam, anche se elementare. È allo studio l'implementazione di un sistema antispam centralizzato per la rete.
8	9	2	M	Filtrare il contenuto del traffico web.	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro, tramite l'adeguata configurazione del sistema antivirus. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
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).	E' stata data disposizione agli operatori di configurare in tal senso le postazioni di lavoro, tramite l'adeguata configurazione del sistema antivirus. Il responsabile della transizione al digitale verificherà regolarmente il rispetto di questa disposizione.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	N.N.
8	11	1	S	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.	N.N.

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.	In corso di implementazione. Attualmente le copie vengono effettuate manualmente dagli operatori su un dispositivo NAS allocato in sala SERVER inaccessibile ai non addetti.
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.	In corso di implementazione per le applicazioni e il software. Sono previsti diversi punti di ripristino per il S.O.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	È disponibile per i backup un NAS in sala server (chiusa e vietata ai non addetti). È in corso di implementazione un sistema più complesso e adeguato alla struttura delle reti.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	In corso di implementazione.
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.	Si veda il punto 10.1.3.
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.	Si veda il punto 10.1.3.

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 fisicamente controllato e protetto da password.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Il sistema di cifratura utilizzato è quello previsto dai software in utilizzo sia per i dati in locale che per quelli in cloud.
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.	Gli operatori verranno informati in merito ai rischi di operazioni di questo tipo.
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.	N.N.
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.	N.N.
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.	N.N.
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.	I software di controllo di cui alla sezione 8 sono più che sufficienti.

13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	N.N.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	N.N.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Vedi 8.9.2.
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.	N.N.

Firmato digitalmente dal Responsabile
per la Transizione al Digitale
(Dottor Massimiliano Michetti)

MICHETTI MASSIMILIANO

Firmato digitalmente da MICHETTI MASSIMILIANO
Data: 2018.01.02 14:06:16 +01'00'