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	Inventario gestito da Infosapienza per i nodi registrati su IPAdmin; Le risorse allocate presso le ex Vetrerie Sciarra (RM103) non hanno IP statico assegnato (rete servita da DHCP di cui si è richiesto adeguamento a Infosapienza) quindi sono memorizzate per mac address. Le risorse mobili (notebook, tablet) vengono identificate e memorizzate per mac address alla consegna.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Gli inventari di cui al punto 1.1.1 vengono aggiornati quando nuove risorse attive vengono acquistate.
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.	Ealizzato come da 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
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.	Workstation/Laptop (Windows): Windows 7 o successivi, Microsoft Office 2016 (Sapienza)/Openoffice per pc uso comune, Kaspersky Security (Sapienza), Izarc, Google Chrome, Acrobat Reader, VLC, Comodo Backup (pc non di uso comune). Workstation/Laptop (Machintosh): mac OS 10.0 o successivi, Microsoft Office 2016 (Sapienza) o LivreOffice, Kaspersky Security (Sapienza), Izarc, Google Chrome, Acrobat Reader, VLC, Comodo Backup. Server: Windows Server 2012 Essential o successivi/Linux Debian, XAMP, Kaspersky Security (Sapienza), Izarc, Acrobat Reader, Comodo Backup. Su richiesta: Photoshop (Gimp), Acrobat Pro (Ableword)
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Si effettuano verifiche periodiche sui nodi di competenza

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.	SISTEMI WINDOWS CLIENT: 1. creazione di 2 partizioni sull'HD o utilizzo di 2 HD (SSD + trad) per il principio di separazione programmi e dati; 2. installazione da ISO ufficiale del s.o. in C (laddove necessaria); 3. account amministratore con nome particolare e pwd "robusta"; 4. installazione antivirus off-line; 5. richiesta IP o connessione tramite rete wi-fi; 6. impostazioni aggiornamenti automatici di sicurezza; 7. aggiornamenti s.o.; 8. spostamento profili utente su D; 9. installazione sw autorizzato (VEDI 2.1.1); 10. creazione utenze d'uso del pc; 11. controllo disabilitazione account "Guest" per i sistemi non di uso comune; SISTEMI MAC OS X CLIENT: 1. account amministratore con nome particolare e pwd "robusta"; 2. installazione antivirus off-line; 3. richiesta IP o connessione tramite rete wi-fi; 4. impostazioni aggiornamenti automatici di sicurezza; 5. aggiornamenti s.o.; 6. installazione sw autorizzato (VEDI 2.1.1); 7. creazione utenze d'uso del computer. STAMPANTI (MULTIFUNZIONE) DI RETE 1. cambiare la pwd dell'amministratore; 2. impostare IP con il gateway vuoto o con l'IP della stampante e impostare gli IP e/o le sottoreti abilitate all'amministrazione e stampa; 3. abilitare autenticazione e popolare le utenze ; 4. disabilitare stampa/copia pubblica senza credenziali;

					SISTEMI SERVER (operazioni generali): 1. installazione da ISO ufficiale del s.o. in configurazione MINIMALE; 2. account amministratore con nome particolare e pwd “robusta”; 3. creazione account d’uso; 4. richiesta IP; 5. impostazioni aggiornamenti automatici di sicurezza; 6. aggiornamenti s.o.; 7. attivazione servizi autorizzati e installazione sw autorizzato (VEDI 2.1.1).
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Secondo specifiche 3.1.1
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Configurazioni 3.1.1 memorizzate offline
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini dei OS Microsoft (licenze campus) vengono fornite e distribuite da CINFO o acquistate con l’elaboratore. Le immagini dei sistemi operativi Linux e relative ISO di appliance vengono reperite direttamente dai siti ufficiali di distribuzioni. L’immagine standard del sistema viene ottenuta tramite clonezilla.
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).	Per la connessione al server viene utilizzato Desktop remoto (da sottorete autorizzata) e SFTP.

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.	Misura coperta limitatamente ai sistemi operativi con l'installazione della soluzione AV Kaspersky fornito da CINFO. Per la ricerca di vulnerabilità sulle applicazioni si usa nessus home version.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	vedi 4.1.1
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti sono automatizzati limitatamente alle postazioni di lavoro. In ambito server (appliance) vengono installate automaticamente solo patch critiche e di sicurezza (security updates)
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 air-gapped.
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.	Per quanto riguarda i Sistemi obsoleti (qualora non posano essere dismessi) installazione minimale: solo servizi e software strettamente necessari; disconnessione dalla rete (se possibile), altrimenti restrizioni degli IP e utenze con cui accedere; utenza/e di accesso con privilegi minimi; scambio di dati tramite memorie/usb pen dedicate; scansione prima e dopo l'utilizzo delle memorie/usb pen sui sistemi a 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.).	Priorità di risoluzione criticità: server di dipartimento, server secondari, amministrazione, segreteria didattica, responsabili di sezione o scuola, personale docente, personale non docente, terminali di pubblico utilizzo. Laddove non sia possibile la risoluzione si proceda come in 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.	Come da piano definito in 4.8.1, priorità all'integrità dei dati e al blocco della diffusione tramite disconnessione dalla rete.

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.	Sulle postazioni di lavoro in uso a laboratori o centri calcolo, laddove possibile, usati solo utenti non amministratori. Si evita di fornire privilegi amministrativi a personale che non abbia necessità operativa di modificare la configurazione.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Sulle postazioni di lavoro in uso a laboratori o centri calcolo usati solo utenti non amministratori, e usati i privilegi amministrativi quando è necessario. Laddove possibile registrati gli accessi effettuati dalle utenze amministrative tramite log file di sistema. Su pc in uso ad utenti limitato l'uso di utenti non amministratori e uso dell'account amministratore solo in caso di effettiva necessità. Sulle console di gestione delle stampanti limitato solo agli amministratori dell'accesso come amministratore, eventualmente creati ulteriori utenti per la gestione con privilegi più bassi laddove il software lo consenta .
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Redatto un documento in cui inventariare le utenze amministrative, a chi sono in possesso e su quali dispositivi, consegnato al Direttore del Dipartimento.
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.	Ad ogni dispositivo collegato alla rete vengono sostituite le credenziali di default secondo procedura 3.1.1
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).	Adozione e promozione della password policy di Sapienza (https://web.uniroma1.it/infosapienza/sites/default/files/passwordpolicy.pdf)
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Impostazione scadenza password secondo password policy Sapienza
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Vedere 5.7.1
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Vedere 5.2.1 e procedura descritta in 3.1.1
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze amministrative sono sempre registrate e sempre riconducibili, in termini di responsabilità, ad una persona fisica.

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.	Riconducibilità garantita da 5.2.1 e 5.10.2; ogni intervento tramite utenze amministrative anonime viene segnalato e ne viene tenuto log.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Predisposte le utenze amministrative su un documento (foglio password) garantendone la riservatezza e consegnarlo al direttore di dipartimento.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non utilizzati certificati digitali per l’autenticazione

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.	Misura coperta dall'installazione dell'antivirus (campus) fornito da CINFO a tutte le strutture reperibile su https://campus.uniroma1.it
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i dispositivi è installato ed abilitato il firewall locale
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Coordinamento con il RUP, verifica di ogni richiesta IP e acquisto
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Disattivata su sistema operativo
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Disattivata su sistema operativo laddove non necessaria
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Vedi 8.1.1. L'interfaccia web di Google Mail non consente l'apertura automatica di messaggi di posta, ne consente la visualizzazione di anteprima , senza esecuzione di codice
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Disattivata da Antivirus
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Impostata da Antivirus
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.	Filtro settato su Antivirus
8	9	2	M	Filtrare il contenuto del traffico web.	Filtro settato su Antivirus
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).	Filtro settato su Antivirus

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.	Il backup delle postazioni e dei dati viene effettuato con la cifratura e accesso tramite password dal software Comodo Backup.
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.	Comodo Backup garantisce cifratura del file di 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.	Vedi 10.1.1

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	Tutte le copie di sicurezza dei dati sono crittografate.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Misura coperta dalla presenza del firewall perimetrale laddove presente. CINFO a seguito di segnalazione del GARR opera un blocco del traffico agendo sul protocollo o sulla porta