MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITA' E RICERCA - REGIONE SICILIANA
ISTITUTO COMPRENSIVO "SAN GIOVANNI BOSCO"
e-mail agic85300c@istruzione.it pec: agic85300c@pec.istruzione.it cod. fiscale 82002930848
Cod. Mecc: AGIC85300C sez. ass.te: AGMM85301D- AGMM85302E-AGEE85301E-AGEE85302G-AGAA853019-AGAA85302A-AGAA85303B
Via Dante, 18 CAP 92028 NARO (AG)
tel. 0922/956081 –Fax 0922/956041 - Codice Univoco Ufficio: **UF0LEP**
Sito Web: https://www.icsangiovannibosconaro.gov.it

ISTITUTO C. - "S.G. BOSCO"-NARO
Prot. 0006057 del 29/12/2017
A-32 (Uscita)

APPLICAZIONE CIRCOLARE N. 2/2017 AGID

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	Realizzato un archivio delle risorse attive, Azione da fare: un elenco dei dispositivi utilizzati dall'amministrazione in tutti i suoi plessi collegati alla rete dati. L'archivio potrebbe essere così organizzato: Nome PC/ Collocazione/IP Assegnato/Applicativi installati /ecc...
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento avverrà quando saranno aggiunte nuove risorse connesse e non alla rete. Azione: modifica elenco vedi 1.1.1
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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 archivio 1.1.1 Azione: Nessuna
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.	Realizzato, tali dati sono inseriti nell'archivio delle risorse attive di cui al punto 1.1.1 Azione: Nessuna
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

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.	Realizzato in seno al documento programmatico sulla privacy 2017-2018 Azione: Fare un elenco dei software utilizzati su ogni macchina. Sistemi operativi windows xp-7-10, sono istallati applicativi Argo software per la gestione di contabilità-inventario-emolumenti-alunni -personale risulta istallato l'antivirus e firewall Kasperski sui pc in dotazione agli uffici e presidenza . Estendere istallazione Antivirus che si aggiorni automaticamente anche alle altre apparecchiature entro il 31.12.2018
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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).	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodicamente saranno realizzate dei controlli per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1. Azione: Periodicamente, non è specificato un minimo, va verificato che non siano installati nuovi software, se questo avvenisse perché necessari all'amministrazione va aggiornato l'elenco al punto 2.1.1.

					aggiornata la versione del documento e firmato digitalmente. I precedenti documenti vanno comunque conservati, perché certificano le misure intraprese nel tempo per garantire i minimi di sicurezza.
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.	Prassi già in uso Azione:nessuna
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema software specifico

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.	Prassi già in uso AZIONE: nessuna
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
3	2	1	M	Definire ed impiegare una configurazione standard per	Nel caso in cui un dispositivo risulti compromesso sarà ripristinato

				workstation, server e altri tipi di sistemi usati dall'organizzazione.	alla configurazione standard. Se un virus o qualunque azione malevola infetti la macchina questa va riformatta e portata ai valori standard o se previsto ripristinare una immagine precedente. possibile l'utilizzo di macchine virtuali di emergenza.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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 le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri, quindi chi svolge manutenzione ai dispositivi o che offre assistenza ai software installati nel caso di accesso remoto dovrà fornire assistenza solo utilizzando protocolli sicuri e criptati.
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

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.	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei dispositivo Eseguire quindi scansioni manuali con il Software Antivirus ad ogni aggiornamento significativo (es. Service Pack o Fix di sicurezza) o almeno una volta all'anno. Aggiornare l'elenco alla voce data aggiornamento del punto 2.1.1
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Azione: verifica trimestrale
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).	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

				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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	I software di ricerca della vulnerabilità sono regolarmente aggiornati. Azione: Verificare che il software Antivirus abbia attivato l'aggiornamento automatico.
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	Servizio già fornito dall'antivirus Kasperski Azione: nessuna
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni (se previsto) sono configurati per avvenire in automatico, bisogna però verificare che ogni postazione abbia attivi gli aggiornamenti automatici del sistema e dei software installati
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.	Sarà garantito l'aggiornamento anche ai dispositivi air-gapped. se eventualmente presenti nella lista al punto 1.1.1. si procede ad un aggiornamento manuale e periodico ai dispositivi non connessi alla rete per cui non è possibile impostare l'aggiornamento automatico.
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.	Azione : Da realizzare entro 31.12.2018
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 caso si fossero riscontrati dei problemi questi saranno risolti attraverso l'installazione di patch o in ultima analisi ripristinando il dispositivo dichiarato vulnerabile dal software di scansione con le risorse a disposizione (immagini, macchine virtuali

					, reinstallazione s.o).
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.	Azione: verifica trimestrale
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.).	Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione Azione: Garantire che siano state attivate tutte le azioni elencate in questo Vademecum..
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.	Il pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza. Azione: Nessuna
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.	Azione : Da realizzare entro 31.12.2018
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.	Azione : Da realizzare entro 31.12.2018

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.	Si sta procedendo a verificare che l'accesso ai dispositivi da parte degli utenti non avvenga con accessi amministrativi e ove lo fosse a convertire l'utenza in una non amministrativa Azione: Attivarsi affinché gli account utilizzati per accedere al dispositivo non siano di di tipo amministrativo. Nel caso lo fossero questi vanno cambiati con accessi di livello più basso.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni	L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione.

				accesso effettuato.	Azione: Come specificato in risposta
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Prassi organizzativa già in uso Azione: nessuna
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Prassi organizzativa già in uso Azione: nessuna
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Predisporre un elenco degli utenti amministrativi e relativa password assegnata. Tale elenco dovrà essere custodito in cassaforte e messo a disposizione solo al personale addetto alla manutenzione dei dispositivi. Le password dovranno essere non banali e di almeno 14 caratteri di lunghezza. Queste utenze saranno aggiornate periodicamente e nell'elenco sarà indicata la data di ultima modifica e le precedenti password. Ove possibile ogni dispositivo dovrà avere solo un utente con privilegi amministrativi. Predisporre un elenco anche per le utenze non amministrative, con relativi moduli e password conservate in luogo sicuro
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Dopo l'installazione di un nuovo dispositivo verrà cambiata la password di default dell'utente amministratore con una utenza amministrativa predisposta come al punto 5.2.1
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

				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 password utilizzate per le utenze amministrative sono lunghe almeno 14 caratteri e non banali Vedi punto 5.2.1
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le password per le utenze amministrative saranno periodicamente aggiornate come previsto al punto 5.2.1
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le password per le utenze amministrative non saranno riutilizzate a breve distanza di tempo Azione: Garantire che le password per le utenze amministrative siano sempre diverse tra loro.
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.	Da realizzare entro 31.12.2018
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.	Si assicura che c’è la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori. Controllo garantito se implementata l'azione 5.1.1
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze amministrative hanno come utente Administrator riconducibile ad uno schema riportato all'elenco riportato alla voce 5.2.1
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o	Le utenze amministrative anonime saranno utilizzate solo per

				"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.	situazioni di emergenza e da chi è autorizzato ad utilizzarle. vedi elenco 5.2.1.
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).	Prassi già in uso Azione:nessuna
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate in un luogo sicuro Azione: Vedi azione 5.2.1
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano per l'accesso certificati digitali Azione: Nessuna, visto che nessuna scuole dovrebbe avere questo tipo di accesso

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 dispositivi sono installati sistemi atti a rilevare la presenza e bloccare l'esecuzione di malware e sono aggiornati automaticamente. Vedi azione 2.1.1
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Ogni dispositivo ha attivo un servizio Firewall come da s.o e un minimo di IPS. In futuro si implementeranno su progetto anche sistemi firewall con IPS evoluti tramite degli hardware appositi
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
8	2	3	A	L'analisi dei potenziali malware è effettuata su di	Attività posta in essere dall'antivirus Kasperski in dotazione

				un'infrastruttura dedicata, eventualmente basata sul cloud.	Azione: nessuna
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è consentito l'uso di dispositivi esterni nella rete amministrativa Azione: Impedire l'uso di dispositivi non scolastici nella rete amministrativa, per svolgere funzioni amministrative
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Attività posta in essere dall'antivirus Kasperski in dotazione Azione: nessuna
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Disattivata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. In ogni caso il software antivirus rileva la presenza di qualunque contenuto in esecuzione automatica o l'esecuzione, come macro, allegati di posta elettronica e messaggi, apertura di immagini e di qualunque altro contenuto
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Vedi 8.7.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Vedi 8.7.1
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Vedi 8.7.1

8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Azione attivata sugli antivirus installati sui dispositivi facenti parte dell'elenco al punto 1.1.1
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.	Attivare il filtro antispam del programma di gestione della posta elettronica. Nel caso di visualizzazione posta direttamente dal sito web, valgono le regole del punto 8.7.1
8	9	2	M	Filtrare il contenuto del traffico web.	Sarà installato entro il 31.12.2018 un proxy server che garantisca il filtraggio del contenuto del traffico web Azione: La scuola si dovrà dotare di un Proxy Server in grado di filtrare il traffico web, ci sono molte soluzioni gratuite che impiegano vecchi PC (es. IPCOP, Smoothwall, ZeroShell, ect.) e che consentono di alzare il livello di sicurezza senza costi per l'amministrazione.
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).	Bloccata nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa. Vedi punto 8.9.2
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema software specifico

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.	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto.
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.	Prassi organizzativa già in uso Azione: nessuna
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Prassi organizzativa già in uso Azione: nessuna

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 operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto. (Applicativo: Gecodoc).
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 punto 10.3.1

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	I dispositivi operano con applicativi Argo software che memorizzano i dati sul cloud per cui non è necessario implementare tale punto Azione: Nessuna
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Prassi organizzativa da adottare entro 31.12.2018 Azione: verifica mensile
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.	I dispositivi operano con applicativi Argo software che memorizzano i dati sul cloud per cui non è necessario implementare tale punto Azione: Nessuna
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.	I dispositivi operano con applicativi Argo software che memorizzano i dati sul cloud per cui non è necessario implementare tale punto Azione: Nessuna
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema

				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.	hardware e software specifico
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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall. Vedi punto 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.	Da realizzare entro 31.12.2018 attraverso l'acquisto di sistema hardware e software specifico

Naro, 29/12/2017

Il Dirigente Scolastico
Dott. Roberto Navarra