ISTITUTO D'ISTRUZIONE SUPERIORE STATALE
"Jacopo del Duca – Diego Bianca Amato" – Cefalù

I.I.S.S.DEL DUCA –.AMATO CEFALU'
Prot. 0017414 del 27/12/2017
01 (Uscita)

ALLEGATO 2
MISURE MINIME SULLA SICUREZZA INFORMATICA

Il Dirigente
Prof.ssa Giuseppina Battaglia

L'Amministratore di Rete
Dott. Ing. Giuseppe Bono

Cefalù 27 Dicembre 2017

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 Implementare ABSC 1.1.1 attraverso uno strumento automatico	La Scuola è dotata di un server / Firewall in ogni plesso che permette l'accesso suddiviso in due modalità che sono: • Dispositivi mappati con Mac Address e nome del Computer • Dispositivi che accedono ad internet tramite nome utente e password e il sistema associa il nominativo che accede associandolo al mac address del device e all'indirizzo IP che viene assegnato al server .
1	1	2	S		L'inventario dei dispositivi mobili che accedono ad internet nella scuola non può essere gestito con una lista premappata in quanto i docenti e il personale varia continuamente con le supplenze e con le rotazioni e quindi si è preferito dare un userID e Password all'utente che accede in modo da mappare il Device dell'utente automaticamente associandolo all'UserId e alla Password dell'utente stesso
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Il sistema istallato presso la Scuola già esegue i log di connessioni dei dispositivi istallati sulla rete e in particolare memorizza IP del dispositivo, mac address del dispositivo e nel caso di accesso al web lo associa alla persona che sta navigando. Nel caso di anomalie il sistema ha degli allert che segnala a video all'amministratore di rete e lo notifica per mail
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Il sistema istallato prevede un analisi di traffico dati dei dispositivi connessi alla rete
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Già Implementato sulla rete. La rete prevede un DHCP con un log di almeno 6 mesi nelle seguenti sottoreti. 192.168.150.X e 192.168.151.x . Sottoreti multiple per consentire l'accesso a tutti i dispositivi autorizzati
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Log già implementato che memorizza tutti i dispositivi sulla rete
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati	Il log dei dispositivi è sempre in real time che permette al bisogno di estrapolare l'inventario in tempo reale. La scuola non ha un

				vengono collegati in rete.	inventario statico in quanto i dispositivi connessi alla rete variano ogni giorno in funzione dei docenti e degli studenti abilitati in funzione delle esigenze didattiche.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Il log dei dispositivi è sempre in real time che permette al bisogno di estrapolare l'inventario in tempo reale. La scuola non ha un inventario statico in quanto i dispositivi connessi alla rete variano ogni giorno in funzione dei docenti e degli studenti abilitati in funzione delle esigenze didattiche.
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.	Il log dei dispositivi è sempre in real time che permette al bisogno di estrapolare l'inventario in tempo reale. La scuola non ha un inventario statico in quanto i dispositivi connessi alla rete variano ogni giorno in funzione dei docenti e degli studenti abilitati in funzione delle esigenze didattiche.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario	Sulla rete è attivo il DHCP pertanto l'associazione tra il Device (Mac address) e l'IP avviene in real time e gestito in maniera automatizzata dal server.

				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.	La distinzione tra personale o scolastico viene dedotto dal MAC address e dal nome macchina che viene dato al dispositivo. Inoltre con i dispositivi che si connettono in WIFI è istallato un controller che gestisce i nomi dei device che accedono e il loro traffico di rete anche quello che non va su internet . Il software è il controller UNIFI che registra tutte le connessioni sulla rete oltre al firewall di sicurezza che registra i log e le altre caratteristiche a norma di legge.
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.	I dispositivi sono tutti identificati automaticamente dal controllerdi rete WIFI e registrati sulla Suite Firewall per l'accesso al Web. Si precisa che i dispositivi mobili possono solo accedere tramite wifi e quindi sotto controllo del Sistema WIFI che registra ogni movimento sula rete .
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	E' istallato un sistema di Autenticazione 802.1x con Captive Portal operante sulle porte 80 e 443 . Ogni device che deve accedere alla rete deve necessariamente inserire le credenziali di accesso con qualunque device senza la necessità di impostare preventivamente nulla sul device come previsto dallo standard di autenticazione 802.11x
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Il sistema ha un suo certificato compatibile con gli standard internazionali X 5xx per l'autenticazione del captive portal

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.	I software autorizzati per i device di proprietà scolastiche già sono preinstallati a cura del tecnico, Per i device personali e in particolare i terminali mobili ad uso didattico è consentito l'istallazione software a cura del docente per usi didattici. Per i device personali non è possibile limitare l'istallazione ma la suite software centralizzata limita l'attività dei software che fanno uso della rete e li segnala tramite allert.
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.	La whitelist del sistema è impostata in modalità automatica tramite DNS Guardian e Squib che permette il filtraggio in funzione del livello di protezione e inoltre impostata una white list manuale da completare al bisogno in funzione degli allert.
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).	La whitelist del sistema è impostata in modalità automatica tramite DNS Guardian e Squib che permette il filtraggio in funzione del livello di protezione e inoltre impostata una white list manuale da completare al bisogno in funzione degli allert.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per	La white list non può essere modificate se non dall'amministratore di rete . Inoltre la lista viene aggiornato almeno ogni 4 ore con collegamento alle white list internazionali che garantiscono una lista web automatica sempre aggiornata .

				verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodocamente l'amministratore di rete provvede a consultare i log delle connessioni di rete con l'analisi delle porte utilizzate per rilevare software che si connette alla rete non autorizzato.
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.	L'inventario del software in licenza d'uso viene tenuto dalla DSGA .
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.	Sul Sistema Wireless il controller registra la tipologia di accesso al web e il browser utilizzato nonche il sistema Operativo del sistema che accede al Web e viene aggiornato costantemente
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.	L'architettura di sicurezza della scuola è istallata su Vmware che al suo interno ha due macchine virtuali , una basata su sistema windows che gestisce il controller WIFI e una su base Linux che gestisce il Firewall di Rete il Content Filter e il Captive portal. Periodicamente le macchine vengono salvate al fine di non compromettere le funzionalità dell'ente nel caso di problematiche . La scuola utilizza sistemi Virtualizzati in Cloud locali su piattaforma VWmare Open Source per una maggiore elasticità del sistema e una ridondanza continua.

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 monitorati regolarmente dal Sistema e dall'Amministratore della rete
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle	Le configurazioni vengono controllate periodicamente e viene fatta una pulizia degli account ogni inizio anno scolastico per poter

				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.	eliminare account di docenti/ studenti che non sono più presenti a scuola
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.	Come specificato in precedenza le immagini dei sistemi vengono salvati periodicamente in quanto i sistemi di controllo centrali sono virtuali pertanto le immagini di istallazione sono sempre conservati pronti per essere istallati.
3	2	1	M	Definire ed impiegare una configurazione standard per	Sistemi monitorati regolarmente dalle FFSS

				workstation, server e altri tipi di sistemi usati dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sistemi monitorati regolarmente dal Tecnico e formattati nel caso i sistemi client siano compromessi
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Vengono fatti secondo la procedura prevista dal regolamento informatico
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Si vengono effettuati in locale
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	L'amministratore della rete provvede ad effettuare le immagini e conservarli in sicurezza
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).	L'accesso remoto è consentito all'amministratore di rete che monitora i sistemi attraverso un software con cripta tura a 256 bit con userID e Password e non con sistemi con Desktop Remoto o similari accessibili sono da rete locale.
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.	Sistema Monitoraro e verificato costantemente
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.	Sistema con allert automatico incluso
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.	Esiste un log di connessioni e di modifica disponibile tramite interrogazione dei log da parte dell'amministratore di rete.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni	Non esiste a livello di didattica un sistema di cartelle e file condiviso pertanto non è necessario identificare le cartelle e le sue variazioni. Infatti per la didattica non esiste una cartella condivisa in quanto non è possibile monitorare i cambiamenti dei file e le persone

				sospette del sistema, delle variazioni dei permessi di file e cartelle.	autorizzate. Inoltre è previsto dal sistema ma non attivato una macchina virtuale che permette di creare un NAS virtuale con accesso tramite userID e passe word
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Il Server Di Rete Centrale controlla tutte le configurazioni a livello rete e le modifiche non autorizzato a livello client non permettono l'accesso alla rete
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Il server permette di accedere ai servizi di rete direttamente con le impostazioni di default dei sistemi sia Win che IOS o Android o Linux

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.	Sistemi monitorati regolarmente dall'Amministratore
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Sistema Testato e monitorato periodicamente dall'Amministratore di Rete
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).	Sistema Testato e monitorato periodicamente dall'Amministratore di Rete con apposite utility
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Nel server Centrale è previsto e utilizzato dall'Amministratore di rete
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Nel server Centrale è previsto e utilizzato dall'Amministratore di rete
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Nel server Centrale è previsto e utilizzato dall'Amministratore di rete e analizzati gli attacchi esterni
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.	Sistema Eseguito dall'Amministratore di rete periodicamente
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	Sistema Eseguito dall'Amministratore di rete periodicamente

				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.	Sistema Eseguito dall'Amministratore di rete periodicamente
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	Sistema Eseguito dall'Amministratore di rete periodicamente con allert tramite mail
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Sistema non adatto per la didattica in quanto i client sono dei docenti
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.	Sistema non adatto per la didattica in quanto i client sono dei docenti i monitorati regolarmente dalle FFSS
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.	Sistema Eseguito dall'Amministratore di rete
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.	Sistema Eseguito dall'Amministratore di rete
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.	Sistema Eseguito dall'Amministratore di rete
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.).	Sistema Eseguito dall'Amministratore di rete
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	Sistema Eseguito dall'Amministratore di rete

				critiche.	
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.	Sistema Eseguito dall’Amministratore di 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 nei sistemi in esercizio.	Sistema Eseguito dall’Amministratore di 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.	Le password dell'Amministratore di rete sono utilizzate solo da Tecnici Specializzate
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Ogni accesso viene registrato con apposito log
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	SI
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Sistemi monitorato da Amministratore di rete
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Sistemi monitorati e gestiti regolarmente da DS e DSGA in collaborazione con Amministratore di rete
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Il server di gestione lo permette .
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.	Sistemi monitorati e gestiti regolarmente da DS e DSGA in collaborazione con Amministratore di rete
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Eseguito da Amministratore di rete
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Eseguito da Amministratore di rete
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Eseguito da Amministratore di rete
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Eseguito da Amministratore di rete
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	Eseguito da Amministratore di rete con la possibilità di accesso anche con certificati vari compatibili con il sistema di gestione AGID

				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).	Complessità di 8 caratteri
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Impostata da Amministratore di rete
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Sostituzione password ogni tre mesi
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Sistema impostato di default
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Sistema impostato di default
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Sistema impostato di default
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.	Sistema impostato di default
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.	Sistema impostato di default
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Sistemi monitorati e gestiti regolarmente da DS e DSGA con Amministratore di rete
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Questo è possibile solo per le utenze amministrative ed è regolarmente gestito da Amministratore di rete
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.	Credenziali gestite da Amministratore di Rete
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).	Si
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne	Sistemi monitorati e gestiti regolarmente da DS su busta chiusa

				disponibilità e riservatezza.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Certificato generato da Zero shell

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.	Il server di rete prevede un antivirus perimetrale che non permette l'attraversamento dei virus all'interno della rete e tale strumento si aggiorna automaticamente ogni due ore.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Sistemi istallati
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Log archiviato dal server
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.	I log non sono modificabili
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.	Il sistema antivirus e anti intrusione è centralizzato e registra tutti i log
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Il sistema cloud privato Zeroshell si aggiorna automaticamente sempre in cloud
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	I dispositivi personali vengono utilizzati dai docenti ai fini didattici ed è permesso l'uso come da regolamento scolastico
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Monitorato da server

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.	Abilitati da server
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi	Utilizzati da Amministratore di Rete
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.	Utilizzato come tool del server
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Utilizzato come tool del server
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Monitorato in automatico
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Nei client privati dei docenti non è possibile utilizzare questa opzione
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Nei client privati dei docenti non è possibile utilizzare questa opzione
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Nei client privati dei docenti non è possibile utilizzare questa opzione
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Nei client privati dei docenti non è possibile utilizzare questa opzione
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Effettuata in automatico con antivirus open source
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.	Effettuata in automatico con antivirus open source
8	9	2	M	Filtrare il contenuto del traffico web.	Effettuato da DNS Guarduan
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).	Effettuato da DNS Guarduan
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme,	Effettuato da DNS Guarduan a da Squid Guardian

				tecniche di rilevazione basate sulle anomalie di comportamento.	
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.	Effettuato dal server con il sistema Clawin

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	Sistemi monitorati e gestiti regolarmente da DS e DSGA per la
				almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	parte amministrativa e direzionale
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.	Effettuati da Amministratore di rete
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Effettuati
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Test fatti con backup incrementali
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.	Sistemi monitorati e gestiti regolarmente da DS e DSGA per la parte amministrativa e direzionale
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.	Sistemi monitorati e gestiti regolarmente da DS e DSGA per la parte amministrativa e direzionale e dal fornitore software per la parte di segreteria digitale

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	Sistemi monitorati e gestiti regolarmente da DS e DSGA per la parte amministrativa e direzionale come da manuale e incarico della privacy
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Non vengono trattati questi dati
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.	Il server dispone di sistemi perimetrali di sicurezza
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi	Effettuati scansioni periodiche
				automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Non necessario
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.	Utilizzato Software remoto solo da amministratore di rete
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.	Previsto dal server di gestione
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Log usabile OFFLINE
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Monitorata porta 443
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Sistemi monitorati e gestiti regolarmente da DS e DSGA per la parte amministrativa e direzionale e da Amministratoee di rete per

					l’area didattica
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.	Eseguito con software specifico

Tale documento riporta la sintesi del sistema di sicurezza generale utilizzato presso questa Pubblica Amministrazione in modo da rispettare le misure minime di sicurezza sia dal punto di vista interno che esterno e utilizza un sistema di autenticazione Captive che permette a tutti i device autorizzati di accedere con credenziali di accesso senza che nel dispositivo venga istallato nessun applicativo e senza che venga configurato nessuna scheda di rete o configurazione particolare. Il sistema viene costantemente monitorato dall’amministratore di rete per consentire un tempestivo intervento in caso di anomalie o furti di identità presenti sul sistema.