via Aurelio Saffi, 136 - 21100 Varese
Tel: 0332 210917 Fax: 0332 228129
Web: www.idsinformatica.it
E-mail: info@idsinformatica.it

IDS Informatica S.r.L.

Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

CIRCOLARE AGID 18 aprile 2017 , n. 2/2017.

Luino 17/01/2018 v1.0 rev0
Varese 28/03/2018 v1.0 rev1

Liceo Scientifico “Sereni” Luino
Via Lugano, 24 – Luino

Il presente documento non è il “modulo di implementazione” da firmare digitalmente con marcatura temporale e da conservare dal responsabile legale e dal dirigente designato, bensì l’analisi delle attività da effettuare per raggiungere i requisiti minimi di sicurezza ICT previsti dalla circolare AGID.
Ad implementazioni completate, verrà rilasciato il “modulo di implementazione” previsto dalla circolare AGID.

Descrizione sintetica dei plessi

Liceo Scientifico “Sereni” Luino

Via Lugano, 24 . Luino

Sono presenti due reti separate, una per la segreteria e una per la didattica

1) - rete segreteria

2)- rete ad uso didattico

1) - rete segreteria

la rete è composta da 1 server windows 2012 dedicato alla gestione del dominio e con funzionalità di file server per i documenti della segreteria dai pc del personale impiegato in segreteria e da 1 nas adibito a storage per backup - non presente rete wifi

L’autenticazione dei pc per l’accesso in rete è fornita dall’active directory del server, facente da domain controller per il dominio liceosereni.local

connettività: adsl telecom

2)- rete ad uso didattico con rete wifi dedicata

laboratorio di informatica

connettività: fibra KPNQwest

Le Norme Minime sono realizzabili, ma solo limitatamente a macchine “amministrative”, cioè non utilizzate per ricerca o didattica. Per queste ultime valgono comunque le impostazioni applicabili alla rete intera (firewall e antivirus)

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	non gestito	Valutabile l'installazione su macchina dedicata di software di inventory con scansioni pianificate (1.1.2) in alternativa a gestione manuale
		2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico		
		3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		
		4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		
	2	1	S	Implementare il "logging" delle operazione del server DHCP.		
		2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		
	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	non gestito	valutabile strumento di inventoring automatico (1.1.2) in alternativa alla gestione manuale
		2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		
	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.	non gestito	valutabile strumento di inventoring automatico (1.1.2) in alternativa alla gestione manuale
		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.		
		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.		
	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.		
	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

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

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
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'istallazione di software non compreso nell'elenco.	non presente	verifica tramite manuale o tramite inventory dei software installati, rimozione di quelli non autorizzati. Utilizzo di credenziali che non permettano installazioni non autorizzate
	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.		
		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).		
		3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.		
	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	non previsto	verifica manuale o tramite software di inventory, con scansioni programmate
		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.		
		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.		
	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped1 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.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	gestione standard dominio windows	gestibile tramite policy dominio windows *
		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.		
		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.		
	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall’organizzazione.	gestione standard dominio windows	gestibile tramite policy dominio windows *
		2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	gestione standard dominio windows	gestibile tramite policy dominio windows *
		3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.		
	3	1	M	Le immagini d’installazione devono essere memorizzate offline.	conservate nell’ufficio DSGA	
		2	S	Le immagini d’installazione sono conservate in modalità protetta, garantendone l’integrità e la disponibilità solo agli utenti autorizzati.		
	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).	utilizzato teamviewer,	verificare che teamviewer utilizzi “Trusted Devices”, È possibile utilizzare le vpn, il firewall presente le gestisce.
	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.		
		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.		
		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.		
		4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.		
	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER						
Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.						
ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

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

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
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.	non gestito	gestibile con software di inventory
		2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.		
		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).		
	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.		
		2	S	Verificare che i log regisrtino le attività dei sistemi di scanning delle vulnerabilità		
		3	S	Verificare nei log la presenza di attacchi pregressi condotto contro target riconosciuto come vulnerabile		
	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.		
		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.		
	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	non gestito	Aggiornamento del software di inventory – update per vulnerabilità di sicurezza gestibili con WSUS **
		2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione.		
	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	gestito in maniera indipendente per ogni macchina	gestibile con WSUS
		2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	gestito in maniera indipendente per ogni macchina	gestione indipendente per ogni macchina
	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.		
		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.	non gestito	verifica implementabile con software di inventory o report di WSUS

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ						
Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.						
ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
	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.		
	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.).	non gestito	Redarre elenco apparati di amministrazione con tipologia e rischi. Relazione per valutare impatto del rischio sul lavoro dell'amministrazione scolastica
		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 qeulle più critiche.	gestito in maniera indipendente per ogni macchina	gestibile con WSUS
	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.		
	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.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

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

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
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.	gli utenti della segreteria e della ditattica hanno diritti di domain user.	già correttamente implementato
		2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Log gestito da windows server	implementato dal domain controller
		3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.		
		4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.		
	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Inventario gestito dal manutentore della rete	Formalizzare l'autorizzazione alle utente amministrative, con lettera d'incarico
		2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.		
	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.	gestito da amministratore di rete	
	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.		
		2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.		
		3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.		
	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.		
	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.		
	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).	implementate regole standard dominio windows	gestibile da policy dominio windows
		2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli		
		3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	non gestito	gestibile da policy dominio windows
		4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	non gestito	gestibile da policy dominio windows
		5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.		
		6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

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

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
	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.		
	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.		
	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Presenti 2 utenza amministrative	correttamente implementato
		2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	le utenze amministrative sono utilizzabili da più persone, interne es esterne	creazione di utenze amministrative differenti per gestore server e gestore software applicativi, se figure differenti.
		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.	l'utenza administrator è utilizzata dall'amministratore di rete	vedi punto 5.10.2
		4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).		
	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	gestito da segreteria	
		2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	certificati non utilizzati	

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
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.	installato antivirus autonomo Nod32	
		2	M	Installare su tutti i dispositivi firewall ed IPS personali.	firewall standard di windows	
		3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.		
	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.		
		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.		
		3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.		
	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	non implementato – dhcp su cavo di rete	implementare tramite firewall abilitazione accesso internet previa autorizzazione mac address
		2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.		
	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.		
		2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.		
	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.		
		2	A	Installare sistemi di analisi avanzata del software sospetto.		
	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.		
	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	non gestito	gestibile da policy dominio windows
		2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	gestione standard di microsoft office	gestibile da policy dominio windows
		3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	anteprima non presente	webmail (Nettuno) non ha anteprima automatica delle email
		4	M	Disattivare l'anteprima automatica dei contenuti dei file.	anteprima non presente	webmail (Nettuno) non ha anteprima automatica dei contenuti dei file
	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	gestito da antivirus locale	

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE						
Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.						
ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
	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.	gestito da fornitore servizio ***	
		2	M	Filtrare il contenuto del traffico web.	gestito da antivirus locale	
		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).	non gestito	gestito dal fornitore di posta elettronica. In rete locale gestito da antivirus Eset
	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.		
	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.		

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di Necessità.

ABSC_ID#			Liv.	Descrizione	Stato attuale	Modalità di implementazione possibili
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	backup effettuato con software Telebackup, con immagini complete del sistema	correttamente implementato
		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.	correttamente implementato	
		3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	correttamente implementato, NAS + dischi usb a rotazione	
	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.		
	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.	non gestito	gestibile con cifratura Telebackup
	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.	backup gestito con protocollo FTP, il nas è quindi disgiunto dal resto della rete e non è accessibile	

IDS Informatica - Valutazione implementazione requisiti minimi sicurezza ICT per le pubbliche amministrazioni

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID#			Liv.	Descrizione	Stato attuale	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	non gestito	implementabile con crittografia del server windows
	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti		
	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.		
	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.		
	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.		
		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.		
	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.		
		2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.		
	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.		
	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	gestito tramite opendns	
	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..		

17/01/2018 V1.0 rev0

Nel corso dell'analisi per la valutazione del rispetto dei requisiti minimi ICT, relativamente alla rete della segreteria, è possibile fare le seguenti osservazioni:

1)mancanza di software di inventory che crei un inventario automatico degli apparati di rete e software installati (facoltativo, l'inventario si potrebbe gestire anche manualmente), oltre a segnalare eventuali vulnerabilità

2) si consiglia di dotare la segreteria di un firewall che permetta di implementare un filtro sulla navigazione impedendo l'accesso a categorie di siti potenzialmente dannosi

Aggiornamento 28/03/2018 V1.0 rev1
Comunicato dalla segreteria del Liceo:

Punto 1) sopra citato risolto con installazione del software di inventory "Lansweeper" in relazione a **ABSC 1 e ABSC 2 e ABSC 4**

Punto 2) sopra citato risolto con installazione di firewall Zyxel in relazione a ABSC13

Visto le informazioni aggiornate al 28/03/2018, si ritiene che la struttura informatica della rete della segreteria del liceo Sereni rispetti le misure minime di sicurezza indicate dalla CIRCOLARE AGID 18 aprile 2017 , n. 2/2017.

* 3.1.1 → https://msdn.microsoft.com/it-it/library/jj966251(v=ws.11).aspx

** 4.4.1 →https://technet.microsoft.com/it-it/library/cc645571.aspx

*** 8.9.1 → https://archivio.pubblica.istruzione.it/webmail/manuali/
Manuale_di_utilizzo_del_Servizio_di_Posta_elettronica_personale_scuola20170428_v1_0.pdf
Gestione email di Nettuno PA

Il dirigente, deve allegare al modulo di implementazione finale l'analogo modulo relativo ai software di gestione della segreteria (es. Nettuno, axios, regel ecc..) che viene prodotto dalle relative software house