2023

Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni

Circolare Agid n° 2
del 18 aprile 2017

Istituto
Scolastico Statale
AMERIGO VESPUCCI 2023/2024

	Realizzato da:	Modificato da:	Visto da:	note
DS	X		X	
DSGA			X	
Amministratore di Sistema	X		X	
Animatore Digitale			X	
RSPP			X	
DPO		X	X	

Indice

Premessa

La direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, in considerazione dell'esigenza di consolidare un sistema di reazione efficente, che raccordi le capacità di risposta delle singole amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della pubblica amministrazione, sollecita tutte le amministrazioni e gli organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici.

Al fine di agevolare tale processo l'Agenzia per l'Italia digitale è stata impegnata a rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

L'Agenzia è costantemente impegnata nell'aggiornamento continuo della normativa tecnica relativa alla sicurezza informatica della pubblica amministrazione ed in particolare delle regole tecniche per la sicurezza informatica delle pubbliche amministrazioni la cui emanazione è però di competenza del Dipartimento per la funzione pubblica e richiede l'espletamento delle procedure previste dalla normativa comunitaria per la regolamentazione tecnica.

Pertanto, il presente lavoro, che contiene le misure minime di sicurezza ICT, viene pubblicato, in attuazione della direttiva sopra citata, al fine di fornire un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilità per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro è in grado di offrire.

L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua.

È comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

Introduzione

L'Istituto Statale AMERIGO VESPUCCI ha avviato un potenziamento della propria infrastruttura ICT, al fine di rendere sempre più efficace l'introduzione dell'informatica nella scuola.

In tale contesto non sono mancate le difficoltà legate al complesso sistema delle competenze necessarie per completare al meglio questo processo ed anche la endemica mancanza di fondi ad esso dedicato che spesso inficia sforzi di ben maggiore importanza.

Non da ultimo la particolare organizzazione delle scuole e la mancanza di figure chiave stabili non facilitano la gestione di processi organizzativi che prevedano un massiccio uso delle tecnologie informatiche.

Solo negli ultimi tre anni si è potuto vedere un movimento più deciso nei confronti delle piattaforme ICT anche grazie al progressivo adeguamento al Codice dell'Amministrazione Digitale.

A fronte comunque di un evidente gap sia tecnologico che di competenze l'Istituto AMERIGO VESPUCCI ha comunque mosso i suoi passi decisamente verso la creazione di un modello ICT organico e diffuso anche in considerazione della logistica degli edifici e dei plessi.

Il rischio è valutato come il prodotto dell'impatto del danno per la probabilità dell'evento.
L'impatto[1] è graduato su una scala da 1 a 4:

Valore	Livello	Definizione/criteri
1	Lieve	Il danno è totalmente reversibile; non si verificano perdita o sottrazione di informazioni
2	Medio	Il danno è totalmente reversibile; si verificano limitate perdite di dati comunque recuperabili ma non sottrazione di informazioni
3	Grave	Il danno è solo parzialmente reversibile; si verificano perdite di dati non recuperabili o sottrazione di informazioni
4	Gravissimo	Il danno è irreversibile; si verificano perdite di dati irrecuperabili o sottrazione di informazioni critiche

La frequenza[1] è valutata su una scala da 1 a 4:

Valore	Livello	Definizione/criteri
1	Improbabile	Eventi poco probabili e indipendenti; non sono noti episodi già verificatisi
2	Poco probabile	Il danno si verifica solo in presenza di circostanze particolari; sono noti solo rarissimi episodi già verificatisi
3	Probabile	La vulnerabilità del sistema ICT può provocare un danno anche se non in modo automatico o diretto; è già noto, all'interno dell'Istituto, qualche evento dannoso determinato dalla vulnerabilità del sistema ICT
4	Altamente probabile	Esiste una correlazione diretta fra la vulnerabilità del sistema ICT e il danno da essa causato; si sono già verificati danni per la stessa vulnerabilità rilevata in situazioni simili

[1] DA MANUALE SICUREZZA 2015, AA.VV. e Metodologia COBIT, 2016

Costruzione e logica delle misure minime implementate

In considerazione della strutturazione differente dell'informatica scolastica, intesa come struttura portante dell'organizzazione, occorre considerare che la scuola ricorre spesso nella sua strutturazione applicativa a fornitori esterni che devono pertanto porre in essere a loro volta tutte le misure minime di sicurezza previste:

Nome applicativo	Fornitore	Messa a norma per misure minime
Bilancio e contabilità	*ARGO*	*Si*
Gestione personale	*SPAGGIARI*	*Si*
Gestione Alunni	*ARGO/GSUITE*	*Si*
Sito internet	*ARGO*	*Si*
Registro elettronico	*ARGO*	*Si*
Applicativi a supporto (segreteria digitale, timbrature, ecc.)	*SPAGGIARI/ARGO*	*Si*

FIGURA 1 - TABELLA APPLICATIVI

L'infrastruttura, da quella di rete a quella Hardware è invece gestita internamente anche se con contratti di assistenza, e viene spesso fornita dagli enti locali:

infrastruttura	Tipo contratto	fornitore	Messa a norma per misure minime
Rete lan	*interno*	*Assistente tecnico*	*nd*
Wifi	*interno*	"	*nd*
Connessione	*Telecom*	*fibra*	*si*
Assistenza Sistemistica			

FIGURA 2 - TABELLA INFRASTRUTTURA

In questo panorama piuttosto variegato si è provveduto a gestire le misure minime, ABSC 1, 2, 3 riguardano la gestione aggiornata degli inventari dei dispositivi e dei software e la protezione della configurazione, ABSC 4 l'analisi delle vulnerabilità, ABSC 5 la gestione degli utenti, in particolare degli amministratori, ABSC 8 le misure di protezione contro l'installazione di software malevolo, ABSC 10 la gestione delle copie di backup, ABSC 13 la protezione dei dati come da seguente tabella:

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	La scuola è dotata di un programma inventario, relativo alle risorse attive ed alla strumentazione informatica e di rete installata. .
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	NO

1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	NO
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	NO
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Le operazioni di logging alla rete DHCP interessano soltanto le connessioni Wi-Fi. Sono gestite da un Captive Portal con accesso solo all'interno della struttura.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	NO
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	SI
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	NO
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.	SI
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.	SI
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.	È in corso di attivazione
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.	NO
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	NO

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Accesso con dispositivo non autorizzato	2 x 3 = 6	
Utilizzo della rete non autorizzato	2 X 2 = 4	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	L'installazione dei software avviene previa richiesta e seguendo il regolamento informatico. I profili "standard" accessibili da docenti e studenti e personale ATA non hanno privilegi di Amministratore.
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.	NO

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).	NO
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	NO
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'attività viene svolta periodicamente
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.	NO
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.	NO
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.	NO

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Installazione software non autorizzato con rischi di sicurezza	2 x 2 = 4	
Utilizzo di software non idonei e/o non collegati con le attività lavorative con danno economico	2 X 3 = 6	

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.	Si sono realizzate in considerazioni delle indicazioni dei produttori
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.	Viene svolto un servizio di analisi e pulizia durante la manutenzione ordinaria
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.	NO
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	La configurazione standard viene definita nel regolamento e viene cambiata in occasione di modifiche organizzative o di cambio di software
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	SI

3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	SI
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	SI le copie di sicurezza sono salvate su dischi esterni
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Si le immagini sono conservate in armadi ignifughi
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).	Si tutte le operazioni di configurazione avvengono su sistemi protetti
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.	SI. Su tutte le macchine sono installati software antivirus.
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.	Si i software antivirus generano allarmi automatici
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.	NO
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	NO
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	NO
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	NO

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Utilizzo errato delle postazioni di lavoro e mancata configurazione corretta	2 x 2 = 4	
Perdita di dati a causa di mancati interventi in caso di Data Breach	3 X 1 = 3	

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.	È in corso di attivazione
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	NO
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).	NO
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	NO

4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	NO
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	NO
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.	NO
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.	SI
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	SI
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	SI
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Nelle macchine sono impostati gli aggiornamenti automatici.
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.	SI, è IN FASE DI IMPLEMENTAZIONE SU TUTTI GLI APPARATI
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.	SI
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.	SI
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.	SI
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.).	Il piano viene definito sulla base delle necessità della struttura
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.	SI
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.	NO
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.	NO

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Perdita di dati a seguito mancata correzione falle sul sistema	3 X 1 = 3	

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
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	SI
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.	NO
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	SI
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	NO
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.	SI
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	NO
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	NO
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	NO
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	NO
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	NO
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).	Vengono definite credenziali robuste
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	NO
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	È in corso di attivazione
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	È in corso di attivazione
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	È in corso di attivazione
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	È in corso di attivazione
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.	SI
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.	NO
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	SI
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	SI
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.	SI
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).	NO

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	SI
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	SI

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Accesso a dati aziendali dopo il furto delle credenziali di amministratore	3 x 1 = 3	

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.	SI
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	SI
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	NO
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.	SI
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.	NO
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	NO
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	SI
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	NO
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.	NO
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	NO
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.	NO
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	NO
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	NO
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	È in corso di attivazione
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	È in corso di attivazione
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	È in corso di attivazione
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	È in corso di attivazione
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	SI
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.	SI
8	9	2	M	Filtrare il contenuto del traffico web.	SI
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).	È in corso di attivazione

8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	NO
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.	NO

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Attacco di virus e malware con perdita di dati	3 x 3 = 9	

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.	SI. Viene effettuato un backup mensile su NAS di parte dell'archivio amministrativo.
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.	NO
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	NO
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	NO
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.	È in corso di attivazione
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	SI

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Perdita delle configurazioni e dei backup	2 x 2 = 4	

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	È in corso di attivazione
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	NO
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 sottrazione di informazioni.	NO
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di	NO

				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.	NO
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.	NO
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.	NO
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	NO
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	NO
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	SI
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.	NO

Valutazione del rischio:

Tipo rischio	Impatto x frequenza	note
Intrusione nella rete di malware e virus o bot con rilevante perdita di dati	3 x 3 = 9	

Valutazione del rischio medio

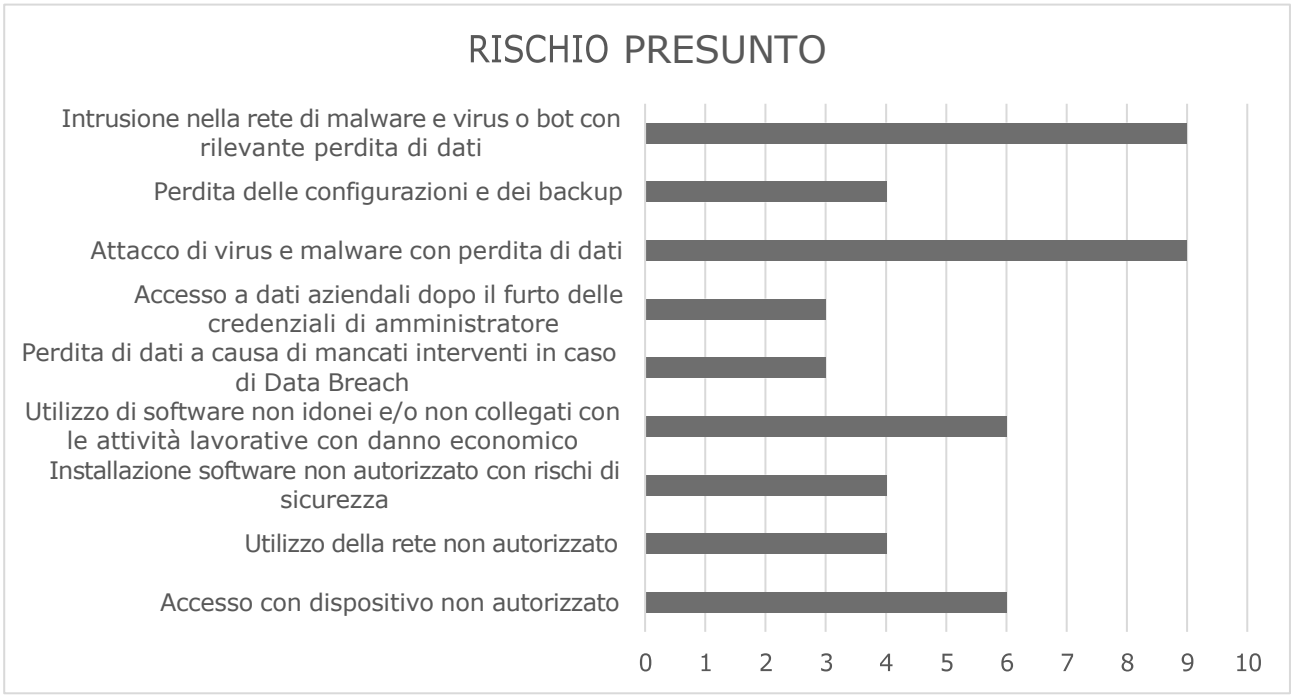

FIGURA 3 - VALUTAZIONE COMPLESSIVA RISCHIO PRESUNTO

Nell'analisi del rischio medio occorre considerare che i valori possibili in cui oscilla l'area di rischio vanno da 1 (basso) a 16 (alto); all'interno di questo range occorre posizionare il rischio medio identificato con le misure minime ed attivare i primi interventi e/o potenziamenti proprio dove il rischio assume valori elevati (vedasi figura 1).

La copertura media del rischio all'attuale data viene riassunta dalla figura 2, che mostra sostanzialmente un'adeguata copertura del rischio possibile:

FIGURA 4 - COPERTURA DI RISCHIO

L'analisi del rischio condotta rispetto ai valori minimi e comunque nel panorama del piano di miglioramento ICT dell'Istituzione Scolastica porta oggi a concentrare l'attenzione sulle misure ABSC 8 e 13, in secondo piano le misure ABSC 3 e 1.

INDICE		Tipo rischio	Impatto x frequenza	note	valore
ABSC	1	**Accesso con dispositivo non autorizzato**	2 x 3 = 6		6
ABSC	1	**Utilizzo della rete non autorizzato**	2 X 2 = 4		4
ABSC	2	**Installazione software non autorizzato con rischi di sicurezza**	**2 x 2 = 4**		4
ABSC	3	**Utilizzo di software non idonei e/o non collegati con le attività lavorative con danno economico**	2 X 3 = 6		6
ABSC	4	**Perdita di dati a causa di mancati interventi in caso di Data Breach**	3 X 1 = 3		3
ABSC	5	**Accesso a dati aziendali dopo il furto delle credenziali di amministratore**	**3 x 1 = 3**		3
ABSC	8	**Attacco di virus e malware con perdita di dati**	**3 x 3 = 9**		9
ABSC	10	**Perdita delle configurazioni e dei backup**	**2 x 2 = 4**		4
ABSC	13	**Intrusione nella rete di malware e virus o bot con rilevante perdita di dati**	**3 x 3 = 9**		9

FIGURA 5 - ANALISI COMPARATA DEI RISCHI

Nella figura 3 appare evidente la mappa delle priorità di intervento per il 2018 a sostegno delle misure minime implementate, ovvero protezione dall'esterno e maggior organizzazione interna.

Conclusioni

Il rispetto delle misure minime è confermato dall'adozione di accorgimenti che, anche se frammentati su più fornitori, garantiscono un primo modello sul quale implementare un'architettura più strutturata.

Nel prossimo biennio l'implementazione del modello ICT si muoverà verso una struttura consolidata con la definizione di un nuovo regolamento che permetterà di avvicinarsi agli standard medi.

I punti di attenzione per l'Istituzione scolastica riguardano particolarmente il potenziamento dei sistemi di difesa della rete e l'ottimizzazione del processo sia di gestione che di configurazione degli apparati e degli accessi.

Altro elemento non di secondaria importanza già indicato in precedenza e la bassa competenza presente in modo stabile nell'Istituzione; a questa problematica sarà necessario far fronte con un attento piano di formazione che dovrà però trovare opportune forme di finanziamento e soprattutto deve avere il carattere della massima diffusione.