MINISTERO DELL'ISTRUZIONE E DEL MERITO
ISTITUTO STATALE COMPRENSIVO *Magistri Intelvesi*
Via Magistri Intelvesi, 11 - 22023 CENTRO VALLE INTELVI (Como)
Tel. 031/830368
CF 80018120131 – Codice Meccanografico COIC80100B
Codice Univoco Ufficio UF0SFC
e-mail: coic80100b@istruzione.it – coic80100b@pec.istruzione.it
sito web: www.icmagistrintelvesi.edu.it

Al **personale scolastico**
All'**Amministrazione trasparente**

MISURE MINIME DI SICUREZZA ICT

Introduzione

Il presente documento determina le misure di sicurezza adottate dall'Istituto Comprensivo Magistri Intelvesi per contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi di piccole e grandi organizzazioni.
La centralità dei sistemi informatici e la crescita esponenziale degli attacchi cui sono soggette anche le Pubbliche Amministrazioni hanno indotto il governo ad affrontare il problema con una serie di provvedimenti a partire dalla **Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015** che impone a tutte le PA l'adozione nel più breve tempo possibile di standard minimi di prevenzione e reazione ad eventi cibernetici. In essa viene individuata nell'Agenzia per l'Italia digitale l'organismo che deve rendere disponibili delle linee guida e degli indicatori degli standard di riferimento cui le PA devono attenersi.
Per assolvere a tale incarico **AGID** ha pubblicato sulla G.U. - Serie Generale n. 79 del 04/04/2017 **la circolare 1/2017 del 17/03/2017** dal titolo ***"Misure minime di sicurezza ICT per le pubbliche amministrazioni"*** sostituita poi dalla ***circolare 18 aprile 2017 n°2***.
In attuazione a tale provvedimento il presente documento specifica le misure di sicurezza adottate dall'istituto scolastico e le modalità con cui esse sono implementate secondo le metodologie e gli strumenti indicati nell'Allegato 1 della circolare AGID.

Il contesto

Prima di procedere a individuare le misure di sicurezza da adottare è necessario definire il contesto in cui ci si trova ad operare. Una qualunque policy di sicurezza non può infatti prescindere dal contesto specifico in cui viene adottata mentre le linee guida di AGID considerano un contesto più generale che è quello delle amministrazioni dello stato così come intese dall'Art. 1. C. 2 del decreto legislativo 30 marzo 2001, n. 165. che cita *istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità' montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale.*

I sistemi informatici dell'istituto sono utilizzati per lo svolgimento dell'attività didattica (PC e LIM nelle classi e nei laboratori) e per lo svolgimento dell'attività amministrativa (PC collocati negli uffici di segreteria a disposizione del personale amministrativo). Data la complessità del sistema informatico, con reti cablate e wireless distribuite su più plessi, e la sua eterogeneità in termini di sistemi, servizi erogati e di utenti (personale docente, personale non docente, alunni) riteniamo sia necessario avvalersi della possibilità indicata dalle linee guida AGID di individuare due sottosistemi caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza cui possono essere associate le due seguenti sottoreti:

Sottorete amministrativa

È costituita dai sistemi utilizzati per lo svolgimento dell'attività amministrativa, per lo più ospitati negli uffici di segreteria e collegati fra di loro da una rete locale cablata. Altri sistemi possono essere utilizzati nelle sedi staccate per lo svolgimento di qualche specifica attività di supporto all'attività amministrativa (rilevazione presenze, postazioni per lo svolgimento di qualche attività di supporto all'attività amministrativa con possibilità di accesso alla email e al sito web istituzionali, etc.). Nella sottorete amministrativa vengono trattati e conservati dati anche di natura personale e riservata.

Sottorete didattica

È costituita dai sistemi utilizzati per lo svolgimento dell'attività didattica presenti in tutte le sedi dell'istituto e comprendente PC collegati alle LIM presenti in tutti i plessi, PC dei laboratori, PC in sala professori, notebook e tablet per un uso in mobilità. I sistemi sono fra di loro collegati, all'interno di ciascun plesso, da una rete locale sia cablata che wireless. Tali sistemi sono usati per lo più come supporto all'attività didattica per cui non è prevista la memorizzazione di dati personali o riservati.

Poiché sarebbe eccessivamente oneroso il raggiungimento di elevati livelli di sicurezza sull'intera struttura informatica dell'istituto, vengono individuati essenzialmente due livelli distinti per le due sottoreti:

Livello di sicurezza sottorete amministrativa: in considerazione dell'attività svolta e delle informazioni trattate si intende adottare e garantire per i sistemi della sottorete amministrativa tutte le misure indicate come minime dall'allegato 1 della circolare AGID. In questa fase, data la limitatezza del tempo a disposizione e la carenza di risorse verranno prese in considerazione le misure di sicurezza AGID definite Standard o Alte solo se immediatamente applicabili in modo semplice.

Livello di sicurezza sottorete didattica: la rete di supporto all'attività didattica presenta notevoli criticità legate ai seguenti fattori:

- **Estensione:** l'attività didattica si svolge su 11 plessi più una sezione distaccata
- **Tecnologia:** le reti locali dell'istituto sono estese agli interi edifici scolastici dei vari plessi con reti eterogenee con tecnologia per lo più cablata e wireless
- **Utenti:** la criticità degli utenti della rete destinata alla didattica è legata essenzialmente al loro notevole numero e alla tipologia (principalmente alunni e docenti con possibilità di accesso in wifi anche ad altro personale scolastico e ad ospiti)

D'altro lato nella sottorete didattica, a differenza di quella amministrativa, non vengono svolte attività critiche dal punto di vista dei dati personali trattati, da tutelare secondo quanto prevede il D. Lgs 196/2003, e di informazioni critiche. Tutto ciò considerato e tenuto conto dell'eccessivo costo in termini economici ed organizzativi, al momento la scuola non è in grado di adottare tutte le misure minime di sicurezza AGID ma si impegna ad adottarne quanto più possibile. Verranno in particolare curati gli aspetti relativi all'uso del Registro Elettronico da parte dei docenti ed il controllo degli accessi ad Internet da parte degli alunni.

MISURE DI SICUREZZA ADOTTATE

Riportiamo di seguito le misure di sicurezza adottate dall'Istituto, individuate secondo la classificazione riportata dalle linee guida della circolare AGID 2/2017. In esse si richiede di specificare gli interventi tecnici ed organizzativi posti in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

A questo proposito si specifica che la gestione del sistema informatico dell'istituto viene condotta da proprio personale interno con il supporto e l'assistenza da parte dell'Azienda che fornisce i servizi di Segreteria digitale e di gestione del Sito web istituzionale; si intende procedere alla nomina di un Amministratore di sistema.

Le linee guida AGID definiscono degli indicatori denominati Agid Basic Security Control (ABSC) ciascuno dei quali è classificato come misura di sicurezza Minima (M), Standard (S) o Alta (A).

ABSC1: 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.

Misure di sicurezza

ABSC 1.1.1 (Liv. M): Implementare un inventario delle risorse attive correlato a quello ABSC 1.4

ABSC 1.3.1 (Liv. M): Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete

ABSC 1.4.1 (Liv. M): Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP

ABSC 1.4.2 (Liv. 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.

Modalità di implementazione delle misure di sicurezza adottate

Realizzazione dell'inventario di tutti i dispositivi hardware collegati alla rete di segreteria con indicazione di:

- Nome identificativo dispositivo
- Tipo di dispositivo
- Persona a cui è stato assegnato
- Collocazione
- Indirizzo IP

L'inventario è tempestivamente aggiornato.

Visti i ristretti termini di tempo la misura è al momento adottata solo nella rete amministrativa ma si procederà ad estendere l'inventario anche a tutte le altre dotazioni hardware dell'istituto.

ABSC 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.

Misure di sicurezza

ABSC 2.1.1 (Liv. 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.

ABSC 2.3.1 (Liv. M): Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

ABSC 2.3.2 (Liv. 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.

Modalità di implementazione delle misure di sicurezza adottate

L'inventario dei dispositivi hardware al punto precedente (ABSC 1) è integrato con le informazioni relative al software comprensivo dei seguenti campi:

- Sistema operativo
- Software installato con relativa versione

L'inventario è tempestivamente aggiornato.

- I sistemi sono soggetti a regolare scansione per rilevare la presenza di software non autorizzato o di software malevolo.

ABSC 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.

Misure di sicurezza

ABSC 3.1.1 (Liv. M): Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.

ABSC 3.2.1 (Liv. M): Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.

ABSC 3.2.2 (Liv. M): Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.

ABSC 3.3.1 (Liv. M): Le immagini d'installazione devono essere memorizzate offline.

ABSC 3.4.1 (Liv. 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).

Modalità di implementazione delle misure di sicurezza adottate

Sulla rete destinata alla didattica viene definita una configurazione standard base costituita dai seguenti software:
- Sistema operativo (Microsoft o Linux)
- Antivirus
- Acrobat reader
- VLC
- Applicativo office (Microsoft o open)
- 7zip
- Mozilla
- Chrome
- Software con funzionalità di blocco di pop up
- Software di masterizzazione gratuito

A questi vanno aggiunti eventuali altri software necessari a svolgere compiti specifici (PC collegati a LIM, PC del laboratorio linguistico, etc.). La configurazione standard per ciascuna postazione è riportata nell'inventario software al punto precedente (ABSC 2.1.1).

ABSC 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.

Misure di sicurezza

ABSC 4.1.1 (Liv. 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.

ABSC 4.4.1 (Liv. M): Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.

ABSC 4.5.1 (Liv. M): Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.

ABSC 4.5.2 (Liv. M): Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.

ABSC 4.7.1 (Liv. 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.

ABSC 4.8.1 (Liv. 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.).

ABSC 4.8.2 (Liv. 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.

Modalità di implementazione delle misure di sicurezza adottate

- I sistemi sono soggetti a regolare scansione per la ricerca delle vulnerabilità dei sistemi. I software sono configurati per l'installazione automatica delle patch e degli aggiornamenti.

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

Misure di sicurezza

ABSC 5.1.1 (Liv. M): Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

ABSC 5.1.2 (Liv. M): Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.

ABSC 5.2.1 (Liv. M): Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

ABSC 5.3.1 (Liv. 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.

ABSC 5.7.1 (Liv. M): Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).

ABSC 5.7.3 (Liv. M): Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).

ABSC 5.7.4 (Liv. M): Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).

ABSC 5.10.1 (Liv. M): Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.

ABSC 5.10.2 (Liv. M): Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.

ABSC 5.10.3 (Liv. 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.

ABSC 5.11.1 (Liv. M): Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

ABSC 5.11.2 (Liv. M): Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

Modalità di implementazione delle misure di sicurezza adottate

Per il rispetto di **ABSC 5.11.1** per le utenze della rete amministrativa viene seguita la procedura già prevista dalla legge sulla Privacy (D.L 196/2003) con la conservazione in busta chiusa delle credenziali del personale amministrativo ad opera del custode delle credenziali. La funzione di custode delle credenziali è svolta dal DSGA nominato dal DS responsabile del trattamento.

ABSC 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.

Misure di sicurezza

ABSC 8.1.1 (Liv. 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.

ABSC 8.1.2 (Liv. M): Installare su tutti i dispositivi firewall ed IPS personali.

ABSC 8.3.1 (Liv. M): Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.

ABSC 8.7.1 (Liv. M): Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.

ABSC 8.7.2 (Liv. M): Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.

ABSC 8.7.3 (Liv. M): Disattivare l'apertura automatica dei messaggi di posta elettronica.

ABSC 8.7.4 (Liv. M): Disattivare l'anteprima automatica dei contenuti dei file.

ABSC 8.8.1 (Liv. M): Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.

ABSC 8.9.1 (Liv. M): Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.

ABSC 8.9.2 (Liv. M): Filtrare il contenuto del traffico web.

ABSC 8.9.3 (Liv. 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).

Modalità di implementazione delle misure di sicurezza adottate

ABSC 8.1.1: Su tutti i PC è installato un antivirus con aggiornamento automatico. Risulta inoltre presente software per il rilievo della presenza di malicious software con settaggio per l'aggiornamento automatico.

ABSC 8.1.2: Su tutti i PC, portatili e server Windows è attivato il firewall di Windows

ABSC 8.3.1: non è possibile collegare dispositivi esterni sulla rete cablata senza l'intervento del docente referente informatico

- L'accesso alle reti wifi avviene in seguito alla digitazione della password degli access point uguale per tutti gli utenti e portata a conoscenza di tutto il personale docente. Tutto il personale è stato informato sulla necessità e l'importanza di tenere riservata la password. Gli alunni non sono autorizzati ad accedere alla rete wifi con propri dispositivi personali.

ABSC 8.7.1: è stata disattivata sui PC l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.

ABSC 8.7.2: è stata disattivata l'esecuzione automatica dei contenuti dinamici presenti nei file.

ABSC 8.7.3: è stata disattivata l'anteprima automatica dei contenuti dei file.

ABSC 8.8.1: le postazioni sono configurate per eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.

ABSC 8.9.1: La scuola utilizza il servizio di posta elettronica ministeriale e certificata (PEC) che include il filtraggio richiesto.

ABSC 8.9.2: A monte della rete locale è presente un sistema di protezione firewall con funzionalità di proxy che permette il controllo degli accessi ad internet in base all'utente, il dispositivo, l'ora e ai contenuti.

ABSC 8.9.3: L'antivirus include funzioni di filtraggio che verranno configurate nel caso in cui si dovesse constatare la necessità di bloccare determinate tipologie di file

ABSC 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.

Misure di sicurezza

ABSC 10.1.1: Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.

ABSC 10.3.1: 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.

ABSC 10.4.1: 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.

Modalità di implementazione delle misure di sicurezza adottate

- La scuola adotta un sistema di backup in rete per la copia automatizzata dei documenti e delle basi dati presenti sul server ed altre cartelle specifiche dei PC della segreteria. Si stanno valutando le implicazioni legate alla copia in cloud dei dati consentita dal sistema di backup adottato.

ABSC 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

Misure di sicurezza

ABSC 13.1.1: 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.

ABSC 13.8.1: Bloccare il traffico da e verso url presenti in una blacklist.

Modalità di implementazione delle misure di sicurezza adottate

- I documenti che meritano particolare tutela sono conservati in cartelle criptate del server accessibili mediante password

Il Dirigente Scolastico
Maria Punelli
(*Firmato digitalmente ai sensi del D. Lgs. 82/2005*)