MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÁ E DELLA RICERCA
ISTITUTO DI ISTRUZIONE SUPERIORE STATALE "GALILEI-SANI"
con sezioni associate
LTTF01801P ITIS GALILEI – LTTL01801V ITG SANI
Via Ponchielli - 04100 LATINA - 0773/663325 - 0773/479316 - C.F. 80003040591
www.isgalileisani.it - ltis018006@istruzione.it - isgalileisani@isgalileisani.it PEC ltis018006@pec.istruzione.it
Ente accreditato dalla Regione Lazio per la formazione e l'orientamento ~ Determinazione 10 Febbraio 2015 n.G01083/2015

IL DIRIGENTE SCOLASTICO

VISTO il D.Lgs 165/2001;
VISTA la circolare AGID n. 2 del 18/04/2017
VISTO il D.Lgs 82/2005 (Codice dell'Amministrazione Digitale)
VISTO il D. Lgs 179/2016
VISTA la Nota MIUR n. 3015 del 20/12/2017 avente ad oggetto "Misure minime di sicurezza ICT per le pubbliche amministrazioni".
VISTA la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 (Misure Minime di Sicurezza Ict Per Le Pubbliche Amministrazioni) in particolare le indicazioni sulle misure minime.

ADOTTA

Art.1

Adozione misure minime di sicurezza ICT per le pubbliche amministrazioni –

le **misure minime** di sicurezza ICT al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informatici, ai sensi dell'art. 3 del D. Lgs 82/2015.

Art. 2

Struttura e architettura della rete-

La rete dell'I.I.S "GALILEI-SANI" di Latina è così strutturata:

- 2 collegamenti verso internet
  - VDSL
  - ADSL
- 1 reta LAN gestita da un Firewall che divide la rete in varie LAN senza avere accesso tra di loro

Ogni VLAN gestisce un settore (server; segreteria; didattica (divisa per laboratori), WI-FI (divisa in 3 settori:DOCENTI-ALUNNI-OSPITI)

Per l'accesso ad internet le VLAN sono dirottate (per la loro tipologia) o su la VDSL (rete a 100Mb) e verso la ADSL (rete a 20MB).

I Dati per tipologia sono archiviati su cloud di proprietà della scuola

Art.3

-Valutazione del rischio, misure di prevenzione e rinvio-

La rete didattica e la rete segreterie sono gestite da un server di accesso (active directory windows)
Per quanto concerne la protezione fisica dei dispositivi, gli stessi sono posizionati in un ambiente fisicamente protetto.
La strumentazione (esclusi quelli collegati alla LAN) di ogni singolo laboratorio è affidata ad un responsabile di laboratorio nominato dal Dirigente Scolastico.
Tutti i dispositivi collegati alla LAN vengono gestiti da amministratori di rete.
Tutti i dispositivi delle segreterie vengono gestiti da amministratori di rete.
Il Dirigente Scolastico è supportato dal Team di Rete, dai responsabili di laboratorio e dagli operatori di segreteria.
L'intera rete dell'Istituto è gestita da un antivirus (Panda Endpoint Protection+) sempre attivo

Le misure sono descritte nell'allegato 1"*Modulo implementazione Misure* ***Minime*** *con suggerimenti"* al quale si rinvia.

Il Dirigente Scolastico
Laura PAZIENTI

Latina 27/12/2017

Firmato da:
PAZIENTI LAURA
Codice fiscale: PZNLRA61P56H501W
27.12.2017 13:17:44 CET

ALLEGATO 1 - Modulo implementazione Misure Minime

SI RITIENE SIANO SUFFICIENTI LE MISURE LIVELLO M NOTA MIUR 3015 DEL 20/12/2017

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 quello ABSC 1.4	Tutte le macchine della scuola sono inventariate. L'inventario elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio ed è strutturato nel modo seguente: • *codice identificativo assegnato all'apparato (inventario patrimoniale);* • *descrizione breve del tipo di dispositivo;* • *MAC Address;* • *indirizzo IP (se statico; se invece l'indirizzo IP viene assegnato dinamicamente, verrà attiva la conservazione del log del DHCP server ;* • *Collocazione alla quale è assegnato.*
1	**3**	**1**	**M**	Aggiornare l'inventario quando nuovi dispositivi approvati	L'elenco di cui alla misura 1.1.1 è aggiornato.
1	**4**	**1**	**M**	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Vedi punto 1.1.1.

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'inventario contiene: • *tipologia dispositivo* • *nome del software* • *fornitore e/o marca* • *versione* • *soggetto autorizzante* • *eventuale data di scadenza dell'autorizzazione* L'aggiornamento dell'elenco dei software è a carico del responsabile. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (vedi 5.1.1)
2	**3**	**1**	**M**	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Le scansioni sono schedulate dal software antivirus. Su qualsiasi dispositivo di rete non è possibile da parte degli utenti di installare hardware e software. Le scansioni

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.	L'intera rete dell'Istituto è gestita da un antivirus attivo. Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica. Per la rete di segreteria si prevede oltre a quanto detto al punto precedente un antivirus per la navigazione in rete. Sono utilizzate copie immagine conservate come descritto al punto 3.3.1
3	**2**	**1**	**M**	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi 3.1.1.
3	**2**	**2**	**M**	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sono state date disposizioni ai responsabili di rete.
3	**3**	**1**	**M**	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di ripristino sono salvate su un server imaging. La rete di segreteria opera con software proprietari e quindi non è necessaria l'immagine. Il database e i dati invece sono oggetto di backup ricorrenti a cadenza giornaliera.
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).	La rete didattica è separata da quella della segreteria. Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…).

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.	Giornalmente tutti i dispositivi informatici vengono aggiornamenti attraverso l'esecuzione automatica del Panda Antivirus.
4	**4**	**1**	**M**	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Sono state date disposizioni agli amministratori di rete di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.
4	**5**	**1**	**M**	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'applicazione delle patch di vulnerabilità è schedulata dagli amministratori di rete.
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.	I dispositivi air-gapped sono disabilitati e gestiti dagli amministratori 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.	Sono state date disposizioni agli amministratori 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.).	Periodicamente gli amministratori di rete leggono i log e i report e agiscono in base alla criticità
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.	Vedi 4.8.1 Sono state date disposizioni ai responsabili 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.	La rete didattica e la rete segreterie sono gestite da un server di accesso (active directory windows) solo gli amministratori di rete hanno i privilegi di configurare
5	**1**	**2**	**M**	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutte le informazioni relative agli accessi, di amministrazione e non, ai dispositivi vengono registrate su active directory log
5	**2**	**1**	**M**	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I documenti di nomina dei responsabili di laboratorio e responsabili di rete sono consegnati agli stessi e una copia è conservata in segreteria.
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.	Sono state impartite adeguate istruzioni al riguardo agli amministratori di rete
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).	Agli utenti vengono fornite password generate automaticamente con un minimo di 16 caratteri alfanumerici
5	**7**	**3**	**M**	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)	Agli utenti non è consentito modificare la password.
5	**7**	**4**	**M**	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Vedi punto 5.7.3
5	**10**	**1**	**M**	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Tutte le utenze sono nominative riconducibili ad una sola persona.

5	**10**	**2**	**M**	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Vedi punto 5.10.1
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.	Tutte le utenze di S.O. sono nominative agli amministratori della rete
5	**11**	**1**	**M**	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Già previsto nella Privacy, vengono raccolte in busta chiusa e conservate dal responsabile del trattamento Le credenziali di accesso degli amministratori di rete sono conservate dal responsabile del trattamento. Le credenziali utenti sono conservate in un software di gestione protetto da una password dal responsabile della transizione.
5	**11**	**2**	**M**	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Si utilizzano certificati digitali per l'autenticazione delle utenze di amministrazione se non quelle di sistema.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	**1**	**1**	**M**	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico.
8	**1**	**2**	**M**	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC, portatili, tablet e server di proprietà della scuola è attivato un firewall
8	**3**	**1**	**M**	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Solo ed esclusivamente tramite la rete WI-FI
8	**7**	**1**	**M**	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Tutte le postazioni non hanno la possibilità di installare unità esterne e/o installare software

8	**7**	**2**	**M**	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'utente non essendo amministratore non può eseguire macro all'interno dei file. Solo gli amministratori di rete sono abilitati
8	**7**	**3**	**M**	Disattivare l'apertura automatica dei messaggi di posta elettronica.	La posta elettronica viene gestita da un unico operatore designato dal DSGA e DS
8	**7**	**4**	**M**	Disattivare l'anteprima automatica dei contenuti dei file.	Vedi punto 8.7.3
8	**8**	**1**	**M**	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	La scansione viene automaticamente gestita dall'antivirus.
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.	La scuola utilizza il servizio di posta elettronica ministeriale e certificata(PEC) che include il filtraggio richiesto.
8	**9**	**2**	**M**	Filtrare il contenuto del traffico web.	L'antivirus e il firewall includono funzioni di filtraggio
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).	Vedi punto 8.9.2

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.	Giornalmente vengono eseguite copie di backup per i sistemi sensibili
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.	Tutti i dati vengono salvati su NAS logisticamente posizionati in più luoghi protetti
10	**4**	**1**	**M**	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Vedi punto 10.3.1

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	**1**	**1**	**M**	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Le utenze anche multiple all'interno del dispositivo sono controllate da active directory
13	**8**	**1**	**M**	Bloccare il traffico da e verso url presenti in una blacklist.	Vedi punto 8.9.2