ISTITUTO COMPRENSIVO LUGO 1 “BARACCA”
Via Emaldi, 1 48022 LUGO (RA) - Tel.:0545/22279
e-mail: icbaracca@gmail.com.it ¨ e-mail ministeriale: raic815009@istruzione.it
PEC: raic815009@pec.istruzione.it - sito web: www.iclugo1.gov.it
CODICE MINISTERIALE DELLA SCUOLA: RAIC815009 – CODICE FISCALE: 82003430392

Misure minime di sicurezza ICT per le pubbliche amministrazioni.
(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)

					Min.	Std.	Alto	Modalità di implementazione
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI								
SC_ID #			**Descrizione**	**FNSC**				
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X	Sono inventariati con aggiornamento periodico nell’inventario patrimoniale: PC, notebook, laptop, server, stampanti, fotocopiatrici, tablet, apparati di rete. In tale inventario sono riportate almeno le seguenti informazioni: - codice identificativo univoco assegnato all'apparato (ad es. PC08; oppure l'identificativo del bene assegnato nell'inventario patrimoniale); - descrizione breve del tipo di dispositivo; - collocazioneall'interno dell'Istituto (ufficio o aula).
1	3	1	Aggiornare l’inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X	L’aggiornamento degli elenchi è in carico del Team Digitale dell'Istituto e alla segreteria amministrativa.
1	4	1	Gestire l’inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l’indirizzo IP.	ID.AM-1	X	X	X	Vedi punto 1.1.1.
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI								
2	1	1	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.	ID.AM-2	X	X	X	L’installazione di software è bloccata per tutti gli utenti ad eccezione degli utenti con diritto di amministratore. Eventuali nuovi software sono installati esclusivamente dall’amministratore dopo verifica della tipologia e della funzionalità.
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X	L'Amministratore di Sistema esegue periodicamente la verifica del software installato su ciascun dispositivo. Eventuale software installato che non risulti nell’elenco viene segnalato affinché venga rimosso o, se valutato necessario, mantenuto.
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER								
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X	Non viene effettuata configurazione standard ma tutte le macchine vengono reinizializzate. In genere vengono definiti per ogni macchina due livelli di accesso: uno con diritti di amministratore protetto da password segreta, uno standard senza diritti di amministratore per l'accesso alle attività didattiche protetto da password palese.
3	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall’organizzazione.	PR.IP-1	X	X	X	Le macchine omogenee per tipo e sistema operativo hanno delle configurazioni standardizzate.
3	2	2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X	Sono state date disposizioni agli amministratori di sistema in tale senso.

3	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X	Le immagini di installazione sono memorizzate su supporto ottico o USB rimovibile.
3	4	1	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).	PR.AC-3 PR.MA-2	X	X	X	Le operazioni di amministrazione da remoto sono impedite. In caso di necessità vengono abilitate temporaneamente connessioni attraverso protocolli sicuri e disabilitate al termine dell'intervento.
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ								
4	1	1	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.	ID.RA-1 DE.CM-8	X	X	X	I sistemi Windows Server Update Services (WSUS) e Trend Micro OfficeScan Agent effettuano costantemente una scansione generale delle vulnerabilità su PC e server (fisici e virtuali) connessi alla rete . In caso di modifiche si procede alla riconfigurazione dei firewall e ad una scansione completa dei sistemi.
4	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	DE.CM-8	X	X	X	Gli antivirus sono configurati per l'aggiornamento automatico.
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	PR.MA-1	X	X	X	I dispositivi sono configurati per l'aggiornamento automatico del SO.
4	5	2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X	X	X	Non vi sono sistemi separati dalla rete.
4	7	1	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.	PR.IP-12 RS.MI-3	X	X	X	Sistemi monitorati regolarmente dalle FFSS.
4	8	1	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.).	ID.RA-4 ID.RA-5 PR-IP.12	X	X	X	Esistono procedure automatizzate di backup per la salvaguardia dei dati residenti in sede.
4	8	2	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.	PR.IP-12	X	X	X	Tutte le patch relative a vulnerabilità vengono immediatamente implementate appena disponibili.
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE								
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	PR.AC-4 PR.PT-3	X	X	X	Sono identificati tra il personale un docente (FS) e altri docenti incaricati per le attività di amministrazione.
5	1	2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	PR.AC-4 PR.PT-3	X	X	X	L'accesso alle utenze amministrative è limitato al minimo indispensabile. È in via di estensione una procedura di registrazione degli accessi.
5	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ID.AM-6 PR.AT-2 DE.CM-3	X	X	X	Sistemi monitorati e gestiti regolarmente da DS e DSGA
5	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	PR.IP-1	X	X	X	Le credenziali vengono sostituite prima dell'allacciamento in rete.
5	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	PR.AC-1 PR.AT-2	X	X	X	Le password devono includere lettere maiuscole e minuscole,caratteri speciali e numeri.
5	7	3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	PR.AC-1 PR.AT-2	X	X	X	La frequenza di cambio password obbligatoria per gli amministratori è definita con Group Policy.

5	7	4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	PR.AC-1	X	X	X	Non è possibile riutilizzare password precedentemente utilizzate.
5	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	ID.AM-6	X	X	X	La distinzione è assicurata nella configurazione dei server.
5	10	2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	ID.AM-6	X	X	X	Sono associate a nome e cognome degli utenti ad ogni credenziale di accesso.
5	10	3	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.	ID.AM-6 PR.AT-2	X	X	X	Le credenziali sono disponibili solo per i tecnici autorizzati e per l'Amministratore di sistema.
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X	L’elenco cartaceo delle PWD è custodito in cassaforte ed accessibili solo al responsabile della struttura ed al DSGA
5	11	2	Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	PR.AC-1 PR.AC-2	X	X	X	Non si utilizzano certificati digitali per l’autenticazione delle utenze amministrative.
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE								
8	1	1	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.	DE.CM-4 DE.CM-5	X	X	X	Su tutti i PC, portatili e server è installato l’antivirus Trend Micro OfficeScan con aggiornamento automatico con policy gestita dall'Amministratore di Sistema.
8	1	2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X	Su tutti i PC, portatili e server è attivo il firewall nativo del Sistema Operativo.
8	3	1	Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X	Nel disciplinare del personale è stata data disposizione di limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali. In ogni caso i dispositivi esterni non possono accedere ai servizi di rete locale, ma solo al servizio di navigazione Web. Le attività di BYOD necessarie alla didattica utilizzano canali diversi di collegamento in rete e firewall rispetto a quello amministrativo.
8	7	1	Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X	Le postazioni di lavoro sono configurate in modo da disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X	Le postazioni di lavoro sono configurate in modo da disattivare l’esecuzione automatica dei contenuti dinamici presenti nei file.
8	7	3	Disattivare l’apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X	Le postazioni di lavoro sono configurate in modo da disattivare l’apertura automatica dei messaggi di posta elettronica.
8	7	4	Disattivare l’anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X	Le postazioni di lavoro sono configurate in modo da disattivare l’anteprima automatica dei contenuti dei file.
8	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	PR.PT-2 DE.CM-4	X	X	X	Le postazioni di lavoro sono configurate in modo da eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.
8	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l’impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X	Il sistema di posta elettronica è configurato in tal senso

8	9	2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X	Il traffico Web è filtrato tramite piattaforma Fortinet, amministrata tramite il sistema FortiManager.
8	9	3	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).	DE.CM-1 DE.CM-4	X	X	X	Sistemi monitorati e gestiti regolarmente da DS e DSGA per la parte amministrativa e direzionale.
ABSC 10 (CSC 10): COPIE DI SICUREZZA								
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X	Viene effettuato giornalmente un backup di tutti i sistemi su unità di memorizzazione esterna e interna per permettere l'eventuale recupero dei dati .
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.	PR.DS-6	X	X	X	Le copie sono cifrate.
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.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X	Le copie vengono duplicate su dispositivi rimuovibili.
ABSC 13 (CSC 13): PROTEZIONE DEI DATI								
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	ID.AM-5	X	X	X	L'analisi è in via di implementazione. Si stà procedendo al trasferimento su servizi cloud garantiti dai fornitori di servizi. È stata richiesta ai fornitori la dichiarazione relativa alle misure implementate.
13	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5 DE.CM-1	X	X	X	Sistemi monitorati e gestiti regolarmente FFSS per l'area didattica. Si stanno implementando i servizi connessi alla gestione delle apparecchiature di cui al punto 8.9.2.

GEMINIANI DANIELA
19.01.2018 16:52:37 UTC