Unione Europea

FONDI STRUTTURALI EUROPEI

PON 2014-2020

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

MIUR

Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la programmazione e la Gestione delle Risorse Umane, Finanziarie e Strumentali
Direzione Generale per interventi in materia di Edilizia Scolastica per la gestione dei Fondi Strutturali per l'Istruzione e per l'Innovazione Digitale
Ufficio IV

Ministero dell'Istruzione, dell'Università e della Ricerca
Istituto Comprensivo Statale di Casatenovo
Via San Giacomo, 20 – 23880 Casatenovo (LC)
Tel. 039.9204798 – 039.9209012 Fax 039.9275894
E-mail Uffici: - LCIC830005@istruzione.it - Sito web: www.comprensivocasatenovo.gov.it
Cod. Mec. LCIC830005 - CF 94033460133

Misure minime di sicurezza ICT per le pubbliche amministrazioni

Finalità del documento

Il documento, predisposto con riferimento alla Circolare MIUR.AOODGCASIS.REGISTRO UFFICIALE(U). 0003015.20-12-2017, persegue i seguenti obiettivi:

- stabilire una baseline comune di misure tecniche ed organizzative irrinunciabili in tema di sicurezza informatica;
- creare uno strumento per poter verificare lo stato corrente di attuazione delle misure di protezione contro le minacce informatiche, e poter tracciare un percorso di miglioramento;
- responsabilizzare il personale scolastico sulla necessità di migliorare e mantenere adeguato il livello di protezione cibernetica nell'Istituto.

Livelli di applicazione

La circolare sopra citata chiarisce che le misure di sicurezza, in funzione della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, possono essere implementate in modo graduale facendo riferimento ai livelli di seguito riportati.
1) **Minimo**: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. *Questo livello può ritenersi sufficiente per gli istituti scolastici*.
2) **Standard**: può essere assunto come base di riferimento nella maggior parte dei casi.
3) **Avanzato**: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni. Per quanto riguarda l'adempimento relativo alla firma del "modulo di implementazione" si ritiene utile evidenziare che lo stesso assume principalmente la veste di uno strumento di lavoro, in grado di fornire una fotografia dello stato attuale del percorso di adeguamento, e una traccia per l'implementazione di un percorso di miglioramento della sicurezza complessiva del sistema informativo dell'amministrazione. Il modulo, che potrà essere firmato digitalmente dal dirigente scolastico, andrà compilato e conservato dalla scuola che dovrà aggiornarlo proprio in funzione dei cambiamenti e dei miglioramenti conseguiti nel tempo.
Pertanto, il documento focalizza l'attenzione solo sul livello MINIMO delle misure di sicurezza indicandone le modalità di implementazione.

Inoltre, per i servizi erogati in rete dai fornitori tramite la loro infrastruttura tecnologica, ospitanti dati dell'istituzione scolastica (il Registro elettronico e la Segreteria digitale) si fa riferimento direttamente al documento elaborato dalla società Medisoft–NUVOLA, in allegato.

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			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'istituto ha predisposto un inventario cartaceo delle attrezzature informatiche contenente i seguenti dati: numero progressivo, indirizzo ip, descrizione della macchina, funzione, responsabile, ufficio associato. L'inventario è reperibile presso l'ufficio del DSGA. Al momento dell'acquisto e dell'inventariazione della nuova risorsa da collegare alla rete, l'inventario sarà tempestivamente aggiornato.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	All'acquisto di un bene collegato alla rete, contestualmente all'inventariazione, si procederà ad aggiornare l'inventario.
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.	L'inventario contiene i dati come indicato nel punto 1.1.1. L'indirizzo IP è indicato nel caso di IP fisso.

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			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.	Per le postazioni ad utilizzo per personale ATA, del Direttore DSGA e del Dirigente sono autorizzati: • tutti i software acquistati o messi a disposizione dal Ministero o da altri Enti e necessari per svolgere le attività gestionali ed amministrative della scuola • software di firma digitale • software di produttività individuale quali foglio elettronico, scrittura testi, presentazioni, data base • antivirus • visualizzatore di file • browser internet. Per le postazioni a disposizione dei docenti: • software di produttività individuale quali foglio elettronico, scrittura testi, presentazioni, data base • antivirus • visualizzatore di file • browser internet • software acquistati necessari per lo svolgimento della funzione docente. Per le postazioni mobili e/o fisse dei laboratori: • software di produttività individuale quali foglio elettronico, scrittura testi, presentazioni, data base • antivirus • visualizzatori di file • browser internet • software didattico. Per le strumentazioni di rete, server, workstation è autorizzato solo il software indicato dal fornitore. Tutti i software installati devono essere aggiornati all'ultima versione stabile. È consentita solo l'installazione di software in possesso di licenza ovvero di software opensource. Nel caso vi sia la necessità di installare software non presente in elenco, la installazione deve essere espressamente autorizzata dal dirigente e l'aggiornamento dell'elenco deve essere propedeutica alla installazione stessa. L'elenco aggiornato dei software autorizzati è conservato in modo cartaceo e disponibile presso gli uffici del DSGA.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodicamente è effettuato un controllo manuale prendendo possesso della singola postazione ed accertando che via sia installato solo software autorizzato.

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			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Per i server, workstation e apparati la configurazione standard è assicurata da parte della ditta che ha effettuato l'installazione o la manutenzione. Per le postazioni in utilizzo al personale le configurazioni standard sono attivate al momento dell'installazione e della messa in esercizio.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	La configurazione standard è definita da parte della ditta fornitrice al momento della messa in esercizio della fornitura.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Il salvataggio della configurazione è effettuato dal fornitore al momento della messa in esercizio. Per i dispositivi differenti da server, workstation e apparati di rete, la configurazione standard è quella derivante da una installazione ex novo.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Al momento della messa in esercizio dei dispositivi quali server, workstation e apparati di rete, è il fornitore ad effettuare l'immagine del sistema e a renderla disponibile su supporto esterno rimovibile conservato dal DSGA.
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).	Le operazioni di amministrazione dei server, workstation e altre apparecchiature di rete sono effettuate direttamente sulla postazione.

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			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.	L'analisi delle vulnerabilità è effettuata dal fornitore al momento della messa in esercizio dei dispositivi. Successivamente alla modifica della configurazione è il fornitore del servizio di manutenzione a rieffettuare l'analisi. Le vulnerabilità rilevate sono riportate in un apposito registro e sono adottati gli opportuni interventi.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	È il fornitore del servizio ad effettuare l'aggiornamento del software prima del suo utilizzo.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Al momento della messa in esercizio i dispositivi sono configurati in modo da consentire l'aggiornamento automatico del sistema operativo. L'aggiornamento automatico dei software è configurato al momento dell'installazione dello stesso.
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 sistemi non collegati alla rete sono manutenuti aggiornati a carico del fornitore del servizio. Non si dispone di sistemi air-gapped.
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.	È il fornitore del servizio che, dopo aver eseguito la scansione delle vulnerabilità, applica le patch ovvero adotta gli opportuni interventi tecnologici. Il fornitore riferisce al Dirigente e al DSGA di eventuali vulnerabilità non risolvibili. E' il dirigente che decide in merito all'accettazione del rischio coerentemente con il piano dei rischi.
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.).	La gestione delle vulnerabilità di server, workstation e apparati di rete è demandata alle aziende fornitrici o alle ditte preposte alla manutenzione. Per le vulnerabilità relative alle postazioni usate dal personale ATA, direttore DSGA e Dirigente si procede con urgenza per la risoluzione. Per gli altri dispositivi l'eliminazione delle vulnerabilità ha carattere di non urgenza e sono risolte compatibilmente con le risorse disponibili.
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.	

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			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.	Il dirigente assegna formale incarico di amministratore dei sistemi a personale in possesso di competenze adeguate e assicura la formazione e l'aggiornamento adeguato. Per i sistemi acquisiti in outsourcing le attività di amministratore sono demandati al fornitore del servizio.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso ai sistemi come amministratore deve essere registrato in modalità automatica su supporto non rimovibile. Laddove tale funzionalità non è disponibile, la registrazione dell'accesso è effettuata su un apposito registro custodito a cura del DSGA. Per ciascun accesso è necessario indicare ora di inizio e fine, motivo dell'intervento e attività svolta. Per i servizi in outsourcing è il fornitore del servizio che assicura analoghe modalità.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Il dirigente redige un registro di tutti i sistemi in uso e per ciascuno di essi l'elenco delle utenze di amministratore. Per ciascuna utenza è indicato il nominativo della persona alla quale l'utenza è assegnata e l'incarico deve essere formalmente accettato. Per i sistemi in outsourcing è il fornitore del servizio che procede in modo analogo.
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.	La sostituzione è effettuata dal fornitore al momento della messa in esercizio del dispositivo.
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).	L'Istituto non dispone di dispositivi con autenticazione a più fattori. Si dispone che le password debbano essere di almeno 14 caratteri contenente maiuscole, minuscole e numeri, o comunque di elevata robustezza (minori caratteri, ma con l'aggiunta di segni speciali).
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le password di dispositivi preposti alla gestione di dati sensibili sono cambiate ogni 3 mesi. Le altre ogni 6.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	La nuova password deve differire dalle precedenti di almeno 6 caratteri.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Gli account di amministratori sono distinti dagli account utente.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutti gli account sono assegnati in modo inequivocabile a una sola persona.
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.	Le password degli account di amministratore predefinito dei sistemi sono custodite dal custode delle password e in mancanza di designazione dal DSGA. L'utilizzo di tali credenziali è annotato in un apposito registro.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password sono custodite dal custode della password e in mancanza di designazione dal DSGA.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non sono utilizzate chiavi private.

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			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.	Tutti i dispositivi sono forniti, se disponibile per il particolare dispositivo, di software antivirus al momento della messa in esercizio a cura del fornitore.
8	1	2	M	Installare su tutti i dispositivi firewall e IPS personali.	Tutti i dispositivi sono forniti, se disponibile per il particolare dispositivo, di software firewall o IPS personale al momento della messa in esercizio a cura del fornitore.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Il personale non è autorizzato a utilizzare dispositivi esterni.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Il fornitore disattiva tale funzionalità al momento della messa in esercizio del dispositivo.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Il fornitore disattiva tale funzionalità al momento della messa in esercizio del dispositivo.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il fornitore disattiva tale funzionalità al momento della messa in esercizio del dispositivo.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Il fornitore disattiva tale funzionalità al momento della messa in esercizio del dispositivo.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Il fornitore predispone tale funzionalità al momento della messa in esercizio del dispositivo.
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.	Non pertinente con le attività dell'Istituto in quanto non si gestiscono mail server.
8	9	2	M	Filtrare il contenuto del traffico web.	Funzionalità predisposta dal fornitore del servizio di rete.
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).	Non pertinente con le attività dell'Istituto in quanto non si gestiscono mail server.

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			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.	La funzionalità è predisposta dal fornitore al momento della messa in esercizio del dispositivo.
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.	I supporti contenenti le immagini sono memorizzati su hd esterni custoditi in armadio chiuso.
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.	I supporti contenenti le immagini sono memorizzati su hd esterni custoditi in armadio chiuso.

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			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	I dati sensibili trattati dall'istituto sono gestiti in outsourcing.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Funzionalità predisposta dal fornitore del servizio al momento della messa in esercizio degli apparati di rete. Previsto aggiornamento in automatico da cloud del produttore degli apparati.

Casatenovo, 31 dicembre 2017

IL DIRIGENTE SCOLASTICO
(dott. Corrado Giulio Del Buono)