UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO-FESR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
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
MIUR

Ministero della Pubblica Istruzione

Istituto Comprensivo Crema Due
via Renzo da Ceri 2/h - 26013 Crema (CR)
Tel: 0373 30115 – Fax: 0373 230287
e-mail uffici: segreteria@iccremadue.gov.it – cric825003@istruzione.it pec: cric825003@pec.istruzione.it

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'inventario sarà conservato presso l'ufficio del dirigente scolastico L'inventario elenca i dispositivi informatici in dotazione all'istituto, 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 - vedi punti 1.2.1 e 1.2.2);* ● *Collocazione e/o persona alla quale è assegnato.*
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'elenco di cui alla misura 1.1.1 sara aggiornato ad ogni nuovi dispositivo L'aggiornamento dell'elenco è a carico dell' amministratore di sistema.

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

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.	L'elenco sarà compilato e conservato presso l'ufficio del dirigente. L'elenco indicherà: ● *tipologia dispositivo* ● *nome del software* ● *fornitore e/o marca* ● *versione* ● *soggetto autorizzante* ● *eventuale data di scadenza dell'autorizzazione* Riguarderà solo i dispositivi della rete di Segreteria. Per la didattica non vi sarà la possibilità di installare software da parte degli utenti.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'amministratore di sistema eseguirà, anche con l'ausilio di software specifici, verifiche semestrali sui pc della rete di Segreteria. Per la rete di Didattica non è necessario in quanto solo gli admin potranno installare e modificare le configurazioni.

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 la rete di didattica si ritengono sufficienti le misure previste dai sistemi operativi utilizzati. Per la rete di segreteria oltre alle misure già previste dai sistemi operativi vengono installati sui client dei software di endpoint protection.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi ABSC_ID 3.1.1.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Verranno utilizzati sistemi di ripristino forniti con i sistemi operativi in uso.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Non si ritiene necessario attivare immagini di ripristino poiché per i laboratori didattici lo stesso può avvenire mediante clonazione di altri HD o mediante un ripristino totale del sistema, tanto perché non esistono dati da preservare nel tempo. La rete di segreteria opera con software proprietari e database delocalizzati rispetto ai quali non è necessaria l'immagine in quanto l'eventuale ripristino da crash è facilmente riparabile mediante l'intervento delle aziende fornitrici. 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).	Per eventuali connessioni remote saranno utilizzati i protocollo SSH e HTTPS.

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	Per la segreteria si utilizzerà il software antivirus in aggiunta al software di scansione vulnerabilità.

				automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Per la didattica non sono necessari software specifici. I responsabili di laboratorio e gli operatori di segreteria sono informati sulla necessità di monitorare tutti i sistemi in rete, a fronte di una significativa modifica (installazione di un sistema o software nuovo, aggiornamento, modifica della configurazione) di uno o più sistemi o software e di comunicare qualsiasi anomalia al dirigente scolastico o all'amministratore di sistema
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Tutti i software di diagnostica e monitoring saranno regolarmente aggiornati prima del loro utilizzo.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti sono automatici per tutti i Sistemi Operativi e Software.
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.	Non sono previsti sistemi separati.

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.	In base ai risultati delle scansioni, saranno poste in essere le adeguate misure di messe in sicurezza o ove non sia possibile
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.).	L'Istituto di concerto con il team digitale e l'amministratore di stileranno un piano di gestione dei rischi connessi all'utilizzo dei sistemi informativi. In assenza si farà riferimento al DPP per la gestione del rischio informatico generale.
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.	Le azioni che saranno previste nel piano di cui al punto ABSC 4.8.1. e saranno stilate sulla base di priorità.

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.	La rete didattica è strutturata in modalità peer to peer ogni pc avrà più account, i privilegi di amministrazione saranno riservati al docente o al responsabile del laboratorio. La rete di segreteria è di tipo client/server con gestione centralizzata delle utenze e relative policy di sicurezza.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Non è necessario registrare gli accessi nella rete di segreteria poiché vi è un rapporto 1:1 tra operatore e dispositivo.

					La rete didattica non presenta tale necessità.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Sarà mantenuto presso l'Istituto un registro delle utenze amministrative per la rete di 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.	Per nuovi computer dedicati alla rete di segreteria saranno disattivate le utenze di default .
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).	Saranno impostati degli adeguati criteri di sicurezza delle password per gli account amministrativi.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Saranno impostati degli adeguati criteri di sicurezza delle password per le utenze amministrative (scadenza temporale)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Saranno impostati degli adeguati criteri di sicurezza delle password per utenze amministrative (cronologia)
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Agli operatori di segreteria e ai responsabili di laboratorio saranno impartite adeguate istruzioni al riguardo.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze di segreteria saranno nominali ed assegnate alla singola persona. Tale livello di protezione non è necessario nella rete didattica, tuttavia, ove possibile si configurerà un account per ogni alunno/classe.
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 delle utenze di default admin saranno disattivate e dove la disattivazione non sia consentita, saranno custodite esclusivamente dalla direzione didattica qualora si rendesse necessario il loro utilizzo (conservare le password in formato cartaceo in luogo protetto)
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Come da punto precedente
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Eventuali certificati saranno conservati su dispositivi esterni.

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	Su tutti i pc in dotazione all'istituto sarà installato un software di protezione ed aggiornato automaticamente.

				locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	
8	1	2	M	Installare su tutti i dispositivi firewall e IPS personali.	Tutti i dispositivi in dotazione all'istituto saranno dotati di software che prevedano funzioni di Firewall e IPS su ogni dispositivo.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Tutti i dispositivi BYOD sono preventivamente autorizzati dalla direzione didattica e registrati nel filtro mac-address del firewall.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Saranno disattivate ove non lo sia già di default, l'esecuzione di contenuti da parte dei dispositivi esterni.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Su tutti i pc della rete di Segreteria sarà disattivata l'esecuzione automatica di contenuti dinamici.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Su tutti i pc della rete di Segreteria saranno disattivate le funzioni di apertura automatica dei messaggi e saranno utilizzato sempre le ultime versioni disponibili dei software installati.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Su tutti i pc della rete di Segreteria saranno disattivate le funzioni di apertura automatica dei messaggi e saranno utilizzato sempre le ultime versioni disponibili dei software installati.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Saranno installati su tutti i dispositivi in dotazione all'istituto software per la scansione automatica dei supporti removibili utilizzati.
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.	Saranno utilizzati software specifici su ogni client di segreteria.
8	9	2	M	Filtrare il contenuto del traffico web.	Il filtraggio sarà eseguito utilizzando firewall e altri software specifici.
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).	Il filtraggio sarà eseguito utilizzando firewall e altri software specifici.

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.	Di tutti i dati non replicabili e necessari al ripristino dei sistemi vengono eseguiti salvataggi automatizzati.
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.	Le copie di sicurezza saranno cifrate durante l'esecuzione delle copie stesse. Una copia dei data sarà conservata in cloud.
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.	A cadenza mensile saranno eseguite delle copie su supporto esterno. Il supporto sarà poi conservato in cassaforte presso la direzione.

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	Sarà applicata una protezione crittografica ai dati maggiormente sensibili.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il filtraggio sarà eseguito utilizzando firewall e altri software specifici.