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

ISTITUTO COMPRENSIVO "ENRICO MESTICA"
Viale Don Bosco, 55 - 62100 MACERATA
tel.: 0733 230336 / 0733 239334 - **fax:** 0733 239334
e-mail: MCIC82800P@istruzione.it - **u.r.l.:** www.istitutomesticamacerata.gov.it
codice fiscale: 80005700432 - **posta certificata:** mcic82800p@pec.istruzione.it
Codice iPA istsc_mcic82800p - **Codice Univoco ufficio** UF0HK9

Prot. n. 8694 I.3 Macerata, 27 dicembre 2017

All'albo on line dell'Istituzione scolastica
Alla Sezione "Amministrazione trasparente"

Oggetto: Misure minime di sicurezza ICT per le pubbliche amministrazioni ai sensi della Circolare AGID 18 Aprile 2017, n.2/2017.

LA DIRIGENTE SCOLASTICA

VISTI il D.L.vo N.297 del 16 Aprile 1994 e successive modificazioni e integrazioni concernente il testo unico delle disposizioni legislative vigenti in materia d'istruzione, relative alle scuole di ogni ordine e grado;
VISTO l'art. 21 della legge 15 marzo 1997, n.59;
VISTO il Regolamento di autonomia scolastica DPR 8 marzo 1999, n.275;
VISTO il CAD - Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale);
VISTA la circolare AGID 18 Aprile 2017, n. 2/2017;
VISTA la nota MIUR n. 3015 del 20/12/2017 ed i chiarimenti in essa contenuti;

RENDE NOTE

le seguenti misure minime di sicurezza ICT relativamente all'Istituto comprensivo Enrico Mestica di Macerata come riportate nei documenti allegati:
- Allegato 1 "Misure minime di sicurezza previste dalla Circolare AGID 18 Aprile 2017, n.2/2017;
- Allegato 2 "Piano di azione IC Mestica Macerata";
- Allegato 3 "Misure minime di sicurezza previste per la segreteria digitale Axios";
- Allegato 4 "Misure minime di sicurezza previste per il registro elettronico Nuvola".

La dirigente scolastica
Prof.ssa Sabina Tombesi

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

ISTITUTO COMPRENSIVO "ENRICO MESTICA"
Viale Don Bosco, 55 - 62100 MACERATA
tel.: 0733 230336 / 0733 239334 - **fax:** 0733 239334
e-mail: MCIC82800P@istruzione.it - **u.r.l.:** www.istitutomesticamacerata.gov.it
codice fiscale: 80005700432 - **posta certificata:** mcic82800p@pec.istruzione.it
Codice iPA istsc_mcic82800p - **Codice Univoco ufficio** UF0HK9

Allegato 1

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

IC ENRICO MESTICA MACERATA

(Circolare AGID 18 Aprile 2017, n.2/2017)

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
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.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione
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.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation,

				server e altri tipi di sistemi usati dall'organizzazione.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.
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).

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione
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.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
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.
4	7	1	M	Verificare che le vulnerabilità emerse dall e scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatt o e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In parti colare applicare le patch per le vulnerabilità a partire da quelle più critiche.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione
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.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
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.
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).
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).

5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad 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.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione
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.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
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.
8	9	2	M	Filtrare il contenuto del traffico web.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazioneed è potenzialmente pericolosa (e.g. .cab).

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
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.

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.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione
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

Livello di riferimento come da nota MIUR 3015 del 20/12/2017 M= Minimo

ISTITUTO COMPRENSIVO "ENRICO MESTICA"
Viale Don Bosco, 55 - 62100 MACERATA
tel.: 0733 230336 / 0733 239334 - **fax:** 0733 239334
e-mail: MCIC82800P@istruzione.it - **u.r.l.:** www.istitutomesticamacerata.gov.it
codice fiscale: 80005700432 - **posta certificata:** mcic82800p@pec.istruzione.it
Codice iPA istsc_mcic82800p - **Codice Univoco ufficio** UF0HK9

Allegato 2

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

PIANO D'AZIONE

IC ENRICO MESTICA MACERATA

A. Valutazione dei rischi e misure di prevenzione e protezione

Nelle tabelle che seguono si riportano le fattispecie per cui sono evidenziate le vulnerabilità ed il livello di gravità che questi eventi comporterebbero. Le vulnerabilità sono di 3 tipi: "NO", per nessuna, "Parziale" e "SI" per vulnerabilità accertata. Il livello di gravità dell'evento è espresso in 3 gradi: basso, medio e alto.

Descrizione rischio	Vulnerabilità	Livello di gravità	Rischi individuabili
sottrazione di credenziali di autorizzazione	parziale	alto	accesso, sottrazione o divulgazione di dati
carenza di consapevolezza, disattenzione o incuria	no	alto	divulgazione, corruzione o distruzione di dati
comportamenti sleali o fraudolenti	parziale	alto	accesso, sottrazione, divulgazione o distruzione di dati
errore materiale	sì	basso	corruzione o distruzione parziale di dati
malfunzionamento, indisponibilità o degrado degli strumenti	sì	alto	perdita di file, corruzione ed indisponibilità del
spamming o tecniche di sabotaggio	parziale	medio	perdita di file, corruzione ed indisponibilità del sistema
accessi non autorizzati a locali/reparti ad accesso ristretto	no	alto	accesso, sottrazione, divulgazione o distruzione di dati
sottrazione di strumenti contenenti dati	no	alto	accesso, divulgazione o distruzione di dati
accessi non autorizzati a locali/reparti ad accesso ristretto interessati da sistemi ICT	no	alto	accesso, sottrazione, divulgazione o distruzione di dati
sottrazione di strumenti contenenti dati	no	alto	accesso, divulgazione o distruzione di dati
eventi distruttivi naturali o	parziale	alto	perdita di file, corruzione ed

artificiali, nonché dolosi, accidentali o dovuti ad incuria			indisponibilità del sistema
guasto ai sistemi complementari (impianto elettrico, climatizzazione, accessi internet, ecc.)	sì	basso	temporanea indisponibilità del sistema, possibile perdita di dati.
errori umani nella gestione della	parziale	alto	accesso, divulgazione o distruzione di dati,
altro evento	sì	non rilevabile	non rilevabili

B. Misure in essere e di cui si prevede l'adozione

Dopo aver analizzato e valutato i fattori di rischio, relativi alle aree e locali, all'integrità dei dati e alle trasmissioni, sono state individuate le misure di prevenzione e protezione più idonee a ridurre o eliminare il rischio stesso.

L'insieme delle misure preventive e protettive riportate nella tabella seguente, costituisce un programma di fondamentale importanza nell'ambito della politica per la Sicurezza, poiché fornisce una guida operativa, che permette di gestire la Sicurezza stessa con organicità e sistematicità. Le misure sono individuate per tipologia che si presentano come:

1.Preventiva laddove si tende a prevenire l'evento dannoso;

2..Obbligatoria per le misure espressamente definite dalla normativa;

3. di contrasto per tutte le misure che inibiscono gli effetti dell'evento dannoso;

4. di contenimento degli effetti per le misure che non possono impedire il verificarsi o inibire l'effetto dell'evento dannoso, ma possono almeno ridurne l'entità.

Per definire uno scadenzario degli interventi l'istituto scolastico ha adottato un criterio di maggior rilevanza rispetto alle fattispecie di rischio da scongiurare. Questa tabella in particolare sarà oggetto di monitoraggio ed aggiornamento per un miglioramento continuo del sistema di sicurezza, è in tutti i casi sottoposta a revisione laddove si ravvisino necessità di intervento o sopraggiunte non conformità.

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
installazione e configurazione sistema operativo server e client che gestisca le procedure di autenticazione	preventiva	accessi indesiderati e non controllati	sì	nessuna
gestione credenziali di autenticazione a livello di sistema operativo e di procedura gestionale preposta al trattamento	preventiva	accessi indesiderati e non controllati	solo password a livello utente senza la gestione delle scadenza e della conformità	gestione scadenza ed assegnazione credenziali mediante policy di dominio ed eliminazione utenti standard per le procedure gestionali
formazione del personale sui rischi, sulle misure disponibili, sulle procedure di conservazione e di ripristino	obbligatoria	accessi indesiderati, danneggiamenti o perdita accidentale, applicabilità dell'intero sistema di sicurezza	sì	nessuna
Antivirus, antispam	di contrasto	danneggiamenti o distruzione di dati, indisponibilità dei sistemi	sì parziale	Verifica periodica della protezione

Firewall e proxy server	di contrasto	danneggiamenti, diffusione o distruzione di dati, indisponibilità dei sistemi	sì	Nessuna
procedure di backup automatizzato	preventiva	danneggiamenti o distruzione di dati	sì	disporre la delocalizzazione dei supporti HD rimovibili
procedura per custodia ed uso supporti rimovibili	contenimento degli effetti	danneggiamenti o distruzione di dati	custodia in luogo protetto	redazione ed applicazione della procedura
procedure di restore e di disaster recovery	contenimento degli effetti	danneggiamenti o distruzione di dati	restore manuale, senza test e procedura per i data base e i documenti in	procedura e test di restore del sistema
organizzazione delle policy di dominio, gestione dei gruppi organizzativi	preventiva	accessi indesiderati e non controllati, danneggiamenti o distruzione	configurazione delle policy e dei gruppi organizzativi	nessuna
gestione di un server di dominio aggiuntivo o in cluster	contenimento degli effetti	indisponibilità dei sistemi	nessuna	disponibilità pc aggiuntivo, installazione e configurazione
attivazione servizi di auditing e monitoraggio	preventiva	non tracciabilità di accessi o attività non consentite o fraudolente	nessuna	attivazione servizi di auditing e monitoraggio
procedura di distruzione dei supporti removibili non più in uso	di contrasto	diffusione non controllata di dati	sì	nessuna
procedura di spegnimento automatico del server in caso di assenza di alimentazione di rete	contenimento degli effetti	danneggiamenti, diffusione o distruzione di dati, indisponibilità dei sistemi	sì	nessuna
procedura di sospensione automatica delle sessioni	preventiva	accessi indesiderati e non controllati	parzialmente	attivazione procedura di sospensione automatica su tutti i pc
verifica funzionale periodica della funzionalità dei sistemi	preventiva	indisponibilità dei sistemi e affidabilità dei dati	sì	verifica funzionale periodica della funzionalità dei sistemi
vigilanza attiva della sede	di contrasto	accessi indesiderati e non controllati	no	nessuna
vigilanza passiva della sede	di contrasto	accessi indesiderati e non controllati	solo durante la permanenza del personale scolastico	nessuna

registrazione accessi	preventiva	accessi indesiderati e non controllati	registro di visita per gli estranei all'amministrazione	nessuna
autenticazione accessi	di contrasto	accessi indesiderati e non controllati	sì	nessuna
custodia in classificatori ed armadi con chiusura	preventiva	accessi indesiderati e non controllati	sì	nessuna
deposito in cassaforte o armadi blindati e/o antifiamma	preventiva	danneggiamenti o distruzione di dati	sì	nessuna
dispositivi antincendio	contenimento degli effetti	danneggiamenti o distruzione di dati, indisponibilità dei sistemi	sì	dotarsi di estintori CO2 specifici per strumenti elettronici
limitazione dell'accesso dei locali ove risiede il server	preventiva	accessi indesiderati e non controllati	sì	nessuna
assegnazione formale di responsabilità ed incarichi	obbligatoria	non applicabilità del sistema di sicurezza	in corso di assegnazione a tutto il personale	nessuna
certificazione delle attività di società esterne	obbligatoria	malfunzionamento o non applicabilità del sistema di sicurezza	sì	nessuna
procedure di restore e di disaster recovery	contenimento degli effetti	danneggiamenti o distruzione di dati	restore automatico a norma dei dati	nessuna
adozione di un manuale di gestione documentale	obbligatoria	malfunzionamento della gestione amministrativa	sì	già adottato dall'Istituto
adozione del manuale di conservazione sostitutiva	obbligatoria	rischio di perdita dei documenti	sì	già adottato dall'Istituto

C . Criteri e modalità di ripristino

Criteri e procedure per il salvataggio	Supporto magnetico/ottico e luogo di custodia delle copie	Procedura di ripristino e pianificazione
Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente sulla base di procedura scritta	Salvataggio in cartella del server	Restore dati, nessuna pianificazione o test di funzionamento
Procedura backup automatico con cadenza giornaliera.	Salvataggio in server	Restore dati come da contratto

Sezione D - Piano di sicurezza informatica (PSI), Disaster recovery (DR) e continuità operativa (CO)

La Direttiva del 16 gennaio 2002 dal titolo "Sicurezza informatica e delle Telecomunicazioni nelle PA statali" raccomanda a tutti gli organi pubblici l'adozione di misure minime di sicurezza, tali da garantire la tutela del loro patrimonio informativo. Il piano di sicurezza informatica è lo strumento strategico fondamentale per tutelare il sistema informativo, le capacità operative dell'IC E. Mestica di Macerata, la sua immagine, la produttività degli operatori e il rispetto degli obblighi di legge. Gli obiettivi che si vogliono conseguire sono di garantire, in accordo con le leggi e le regole interne:

- per le risorse tecnologiche:
  - la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali, tramite la formulazione di appropriati piani di recupero delle funzionalità del sistema;
  - la continuità del servizio a copertura delle esigenze operative della scuola.
- b) per i dati:
  - la riservatezza delle informazioni;
  - l'integrità delle informazioni;
  - la correttezza delle informazioni ritenute critiche per le eventuali conseguenze derivanti da una loro alterazione;
  - la disponibilità delle informazioni e delle relative applicazioni.

Per risorse informatiche da considerare nell'ambito della sicurezza, ci si riferisce a:

- dispositivi tecnologici (computer, terminali, linee di comunicazione, ecc.) il cui danneggiamento fisico può comportare l'interruzione del corretto funzionamento e la conseguente sospensione del servizio;
- sistemi operativi o prodotti software la cui modifica, cancellazione o indisponibilità può comportare l'interruzione del funzionamento e la conseguente sospensione del servizio oppure può comportare la possibilità di accesso e manomissione di dati riservati da parte di personale non autorizzato;
- programmi applicativi la cui modifica o cancellazione può compromettere l'esercizio di alcune funzioni del sistema informativo o alterarne le corrette caratteristiche di funzionamento;
- i dati per i quali si richiedono riservatezza, integrità e disponibilità.

Il Codice dell'Amministrazione Digitale contiene disposizioni importanti relative alla sicurezza digitale, dei sistemi e delle infrastrutture delle PP. AA. (art.51) rimarcando l'importanza di adottare soluzioni di Continuità Operativa e di Disaster Recovery nella gestione dei sistemi operativi automatizzati. I due termini sembrano molto simili, ma vi è una differenza sostanziale, in quanto la prima è riferita all'organizzazione nel suo insieme (e quindi comprende anche le risorse umane, logistiche, i rischi ambientali, ecc.), mentre la seconda è riferita all'infrastruttura tecnico/informatica.

Procedure di Disaster Recovery (c3, lettera b, art. 50 bis del CAD)

Per disaster recovery si intende l'insieme di misure tecnologiche e organizzative dirette a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi a fronte di gravi problemi. I disastri informatici con ingenti perdite di dati, nella maggioranza dei casi, provocano quindi il fallimento dell'organizzazione, per cui investire in opportune strategie di recupero diventa una scelta quasi obbligatoria e il Piano di disaster recovery è il documento che esplicita tali misure. L'attività di backup è un aspetto fondamentale della gestione del sistema informatico dell'IC E. Mestica di Macerata poiché, in caso di guasti, manomissioni o furti assicura che esista una copia dei dati, garantendo, quindi, una ridondanza logico/ fisica di questi ultimi. L'Istituto utilizza sistemi differenti di backup:

1) sempre on-line modalità cloud per i trattamenti informatizzati attraverso gli applicativi in uso (Axios per la segreteria digitale, Nuvola per il registro elettronico);
2) off- site.

Il backup on-site è effettuato sul server presente nell'ufficio di segreteria; l'esecuzione del backup è impostata in maniera automatica e svolta con una periodicità stabilita di una volta al giorno.

Allegato 3

MISURE MINIME DI SICUREZZA PREVISTE PER LA SEGRETERIA DIGITALE AXIOS IN USO PRESSO L'I.C. MESTICA DI MACERATA

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.	I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD). Il sistema Axios Cloud consente le medesime funzionalità.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	I prodotti Axios registrano in automatico ogni accesso effettuato al sistema. Il sistema Axios Cloud possiede un log puntuale di tutte le operazioni effettuate e consente l'accesso allo stesso a qualsiasi richiesta proveniente dall'utente o dalle autorità preposte
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Vedi punto 5.1.1M Anche per Axios Cloud vedi punto 5.1.1.M
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	I prodotti Axios registrano su tabella di log ogni singola operazione effettuata sui dati. La conservazione di tale log dipende dallo spazio presente sul disco del server della scuola e dalle impostazioni fornite dalla scuola stessa sulla grandezza massima del file di LOG. Il LOG gestito da Axios Cloud viene storicizzato ogni 3 mesi e collocato in stato di READONLY. Dopo 12 mesi viene cancellato
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. Axios Cloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utente.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
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.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza	Vedi punto 5.1.4.A L'aggiunta o la soppressione di un'utenza

				amministrativa.	amministrativa sono operazioni che vengono svolte sul DB e quindi regolarmente registrate nel file di LOG. Anche in Axios Cloud l'operazione viene regolarmente tracciata all'interno del file LOG.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
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).	Axios consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite: 1.Verifica o meno del doppio accesso 2.Inserimento data generale di scadenza password 3.Numero di gg massimi per la validità del codice di accesso 4.Numero massimo di gg da ultimo accesso per consentire ancora lo stesso 5.Lunghezza minima del codice di accesso (in questo caso 14) 6.Numero minimo dei caratteri minuscoli 7.Numero minimo dei caratteri maiuscoli 8.Numero minimo dei caratteri numerici 9.Numero minimo dei caratteri speciali In Axios Cloud verranno a breve implementate le stesse funzioni.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	I parametri definiti in Axios al punto precedente (5.7.1.M) consentono di effettuare questo controllo in automatico impedendo di fatto l'utilizzo di credenziali deboli.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Vedi parametri indicati nel punto 5.7.1.M
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza. In Axios Cloud sarà a breve implementata le medesima funzione
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne	

				effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	Axios consente, per le funzioni particolarmente delicate, di inserire un ulteriore codice di accesso. L'utente quindi dopo aver effettuato il login dovrà inserire anche un ulteriore codice di accesso per poter effettuare la funzione scelta.
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La gestione degli amministratori rispetto alle normali utenze viene fatta, in Axios, tramite la gestione dei livelli (1-9 9=amministratore) e le tipologie di accesso per ogni utente/funzione (5.1.1M)
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	In Axios, ad ogni utenze, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi Anche in Axios Cloud le utenze di accesso sono legate a precise anagrafiche presenti nel sistema
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.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Per quanto concerne i prodotti Axios tali credenziali sono gestite all'interno della base dati, l'accesso alla stessa è consentito solo tramite i programmi Axios e quindi secondo le regole di sicurezza enunciate in questo documento. Anche per Axios Cloud vale lo stesso principio con l'aggiunta che la base dati non è in alcun modo accessibile a nessuno se non tramite programmi Axios e quindi secondo le regole indicate nel presente documento.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

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.	Il programma Axios prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola. Il sistema prevede inoltre l'invio automatico a tre indirizzi mail e/o a tre numeri di cellulare, di un messaggio sull'esito dell'esecuzione delle copie. Il sistema di backup Axios prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle. Axios Cloud effettua - Backup del logo delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 8/10 gg
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Per quanto concerne Axios il sistema di backup effettua il salvataggio della base dati. L'installazione dei programmi è possibile in qualsiasi momento dal sito internet di Axios, così come l'eventuale ripristino del motore di database utilizzato (Sybase ver. 8.0.2.4495) Axios Cloud oltre ad esser dotato di un sistema di backup con retention di 8/10gg dei dati ed un sistema di retention di 2/4 gg delle immagini dell'intera infrastruttura e configurato con un sistema di DR Real Time che consente il ripristino di un subset depotenziato dell'infrastruttura madre entro 24/48 ore dal Fault completo del sistema principale garantendo, quindi, la continuità di servizio con uno SLA del 98.98 % circa.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Axios consente alle scuole di poter effettuare, nella medesima sessione di copie ed in modo completamente automatico, oltre alla copia sul disco del server, anche una copia su unità fisica esterna e, qualora la scuola abbia acquistato il servizio, anche un backup cloud che garantisce l'assoluta salvaguardia e recuperabilità dei dati. I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Axios effettua una verifica al termine della creazione del file compresso contenente le copie. La simulazione del ripristino dei dati è comunque buona pratica da adottare con frequenza almeno mensile.

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.	Il backup effettuato da Axios è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha generato. Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios. Axios Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni Axios Cloud sono cifrate protette da protocollo HTTPS.
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 quanto indicato nel punto 10.1.3.A, in particolare è possibile effettuare una copia su un disco esterno, ad esempio, e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server. I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery.

Allegato 4

MISURE MINIME DI SICUREZZA PER IL REGISTRO ELETTRONICO NUVOLA IN USO PRESSO L'I.C. MESTICA DI MACERATA

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.	Nuvola consente di profilare ciascun utente in modo granulare, tramite un sistema puntuale di permessi e profili, al fine di gestire i privilegi per ogni funzionalità del software.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Nuvola registra gli accessi effettuati in modo automatico.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Vedi punto 5.1.1M
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	È possibile controllare tutte le utenze all'interno delle funzioni di Nuvola di gestione degli utenti e dei ruoli, verificando anche la data dell'ultimo accesso.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
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.	

5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
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).	Nuvola obbliga ad impostare una password alfanumerica di almeno 7 caratteri
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	In Nuvola verrà implementata a breve tale funzionalità
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	In Nuvola verrà implementata a breve tale funzionalità
5	7	5	S	Assicurare che dopo la modifica di tali credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l’accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un’utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	

5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	In Nuvola ad ogni utenza corrispondono privilegi diversi e quindi ogni utenza è distinta dalle altre ed ha diverse credenziali.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	In Nuvola ogni utenza è legata ad una singola anagrafica del personale.
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.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	In Nuvola le credenziali sono conservate in forma criptata all'interno della base dati di Nuvola stessa e quindi sono accessibili solo tramite le funzioni di Nuvola.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

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.	In Nuvola vengono mantenuti tutti i backup di qualsiasi momento temporale degli ultimi 5 giorni.Viene inoltre effettuato un backup giornaliero, mantenuto per 1 anno.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	In Nuvola vengono fatti test periodici di ripristino di tutti i dati di un precedente backup al fine di verificare la possibilità di ripristinare l'intero sistema in caso di disaster recovery.

10	1	3	A	Effettuare backup multipli coNstrumenti diversi per contrastar possibili malfunzionamenti nella fase di restore.	In Nuvola i backup vengono effettuati con strumenti diversi e l'integrità dei dati nel backup viene verificato con appositi software automatici.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Vedi 10.1.2A
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.	In Nuvola i backup sono accessibili solo al fornitore del software. La comunicazione tra la produzione del backup e lo storage avviene tramite HTTPS.
10	4	1	M	Assicurarsi che i supporti contenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le copie di sicurezza.	In Nuvola i backup vengono gestiti in storage diversi da quelli dell'infrastruttura di Nuvola.