MISURE MINIME DI SICUREZZA

Questo documento contiene le informazioni riguardanti il solo software Nuvola, in uso presso le scuole per la gestione informatica delle procedure scolastiche.

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.	E' 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	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	

Madisoft SpA
Via Falcone, 5 – Casette Verdini
62010 **POLLENZA** - MC
Tel. 0733 203595
Fax 0733 1772085

Iscrizione R.I. di Macerata 01818840439
Codice Fiscale e Partita Iva. 01818840439
Capitale Sociale €. 50.000,00 i.v.
http://madisoft.it
e-mail: info@madisoft.it

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 8 caratteri incluso un carattere maiuscolo ed un carattere speciale.
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).	Le credenziali scadono ogni 90 giorni dal primo utilizzo e viene richiesto obbligatoriamente la modifica delle stesse.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non possono essere riutilizzate credenziali già usate.
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.	
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 con strumenti diversi per contrastare 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 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.	In Nuvola i backup vengono gestiti in storage diversi da quelli dell'infrastruttura di Nuvola.