

notes

axios
Italia

La circolare AgID del 26 Aprile 2016 in materia di “MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI” deve essere vista come un documento utile a guidare le PA in un processo di conoscenza delle misure di sicurezza e della loro attuazione in base alla struttura delle singole PA.

Nei prossimi giorni uscirà una nota congiunta MIUR/AgID che spiegherà come il documento allegato alla circolare in oggetto e da compilare entro il 31/12/2017, non deve intendersi statico o impositivo, ma uno strumento per valutare la situazione della sicurezza nei sistemi informativi delle scuole e predisporre nel tempo gli adeguamenti necessari. Deve essere quindi visto come una guida alla cultura della sicurezza nelle scuole.

Axios intende da parte sua, con questa comunicazione, aiutare la compilazione del modello nei capitoli di propria competenza (ABSC 5 ed ABSC 10) delegando alla propria rete la consulenza da dare alle scuole per identificare e catalogare le peculiarità di ognuna.

E’ evidente che questo documento, perché generico, non può tenere conto delle singole situazioni che devono essere indicate da ogni singola scuola.

Di seguito i capitoli riguardanti Axios e cosa, a nostro giudizio, dovrebbero contenere come informazioni.

Indicando i pacchetti Axios si intendono tutti i nostri prodotti Windows client/server, con l’indicazione invece di Axios Cloud, tutti i nostri programmi CLOUD (SD, RE e Protocollo)

All’interno della tabella “*ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE*” sono indicate ovviamente tutte le informazioni concernenti i prodotti Axios. E’ importante ricordare come all’interno di tale tabella debbano essere indicati “*Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.*”

Come privilegi di amministratore non si intende solo l’amministratore dei programmi Axios ma qualsiasi altra utenza avente tali caratteristiche, dall’amministratore della macchina a quello di rete e del server.

Le indicazioni fornite quindi devono essere integrate con le informazioni circa la gestione delle utenze sopra descritte. Esistono una serie di programmi free in internet che possono aiutare la scuola nella gestione di tali utenze al fine di rispettare quando indicato nella norma.

All’interno della tabella “*ABSC 10 (CSC 10): COPIE DI SICUREZZA*” devono essere indicati “*Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.*”

Uno degli strumenti più efficaci per garantire la sicurezza delle copie dei dati è sicuramente dato dal poter effettuare un backup su server cloud.

Attenzione però perché questi devono in qualche modo essere certificati ed essere locati all’interno della Comunità Europea, in quanto, all’interno della base dati, sono presenti dati sia personali che sensibili. Non è opportuno quindi utilizzare spazi cloud free, come forniscono molti giganti del WEB in quanto, pur perfettamente funzionanti, non garantiscono sicurezza e locazione geografica dei vostri backup.

Axios propone in questo caso ai propri clienti, al fine di essere tranquilli riguardo ad una procedura di Disaster Recovery, il proprio programma di [Backup Cloud](#), completamente integrato ed automatizzato, che garantisce un elevato standard di sicurezza e protezione oltre ad una collocazione fisica dei server all’interno del territorio nazionale.

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).
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.
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.	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.
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.
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.	Vedi punto 5.1.4.A L'aggiunta o la soppressione di un'utenza amministrativa sono operazioni che vengono svolte sul DB e quindi regolarmente registrate nel file di 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: <ol style="list-style-type: none"> 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
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.
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

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.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	