Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per l'Abruzzo
ISTITUTO COMPRENSIVO STATALE ROSETO 2
64026 - Roseto degli Abruzzi
Sede legale e Presidenza via FONTE dell'OLMO, 56 – TEL. 085/8991182
Sede operativa e Segreteria via A. MANZONI, 258 - TEL. 085/8991220 - telefax 085/8941878

C.F.	Sito Web	E-mail	pec
91043920676	www.icomprensivo2roseto.gov.it	teic84300r@istruzione.it	teic84300r@pec.istruzione.it

Prot. n. 0009542 / 1.4.d

Roseto degli Abruzzi, 29/12/2017

Si premette che:

- ✓ le misure minime di sicurezza gestite direttamente dall'istituzione scolastica sono state integrate con quelle comunicate dai gestori dei pacchetti applicativi in uso:
  - AXIOS ITALIA (pacchetto Axios Gold) con nota prot. 0009541/1.4.d del 29/12/2017 (integrazioni in azzurro)
  - SPAGGIARI PARMA s.p.a. (pacchetti Segreteria Digitale e Classe Viva) con nota prot. 0009540/1.4.d del 29/12/2017 (integrazioni in verde)
- ✓ l'allegato 2 della Circolare n.2-2017 AGID è stato compilato esclusivamente per le sezioni relative al livello M.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Realizzato un archivio generale delle risorse attive. Realizzare un elenco analitico dei dispositivi utilizzati dall'amministrazione in tutti i suoi plessi collegati alla rete dati. L'archivio potrebbe essere così organizzato: Nome PC Collocazione IP Assegnato Applicativi installati
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento avverrà quando saranno aggiunte nuove risorse. Aggiornare l'elenco delle risorse quando si inserirà un nuovo dispositivo utilizzato dall'amministrazione che risulti essere connesso alla 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.	Tali dati sono inseriti nell'archivio delle risorse attive di cui al punto 1.1.1

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

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.	Realizzato un elenco generale. Tra i software installati è presente un Antivirus che si aggiorni automaticamente. Da fare un elenco dei software utilizzati su ogni macchina. Per quelli di sistema basta precisare la versione del Sistema Operativo, mentre vanno elencati tutti quelli installati, compreso l'antivirus.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodicamente saranno realizzati dei controlli per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1. Qualora fossero stati installati nuovi software, perché necessari all'amministrazione, va aggiornato l'elenco al punto 2.1.1. e aggiornata la versione del documento firmato digitalmente. I precedenti documenti vanno comunque conservati, a certificazione delle misure intraprese nel tempo per garantire i minimi di sicurezza.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Per sistemi desktop e server, definire dotazione software standard e criteri di gruppo nel domain controller attraverso l'active directory per gestire le richieste di autenticazione per la sicurezza.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	**E**ffettuare la configurazione tramite domain controller attraverso l'active directory.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso in cui un dispositivo risulti compromesso (da virus o qualunque azione malevola) sarà ripristinato alla configurazione standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari.
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).	Tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessione protetti e sicuri. Avvisare il personale che svolge manutenzione ai dispositivi o che offre assistenza ai software installati, della condizione che un eventuale accesso remoto dovrà avvenire solo utilizzando protocolli sicuri e criptati.

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

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.	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei dispositivi. Effettuare scansioni manuali con Software Antivirus ad ogni aggiornamento significativo o almeno una volta all'anno. È codificata una procedura interna che, a fronte di modifiche della infrastruttura o di aggiornamenti dei programmi, guida lo svolgimento di test per evidenziare possibili criticità.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	I software di ricerca delle vulnerabilità sono regolarmente aggiornati. Verificare che il software Antivirus abbia attivato l'aggiornamento automatico. Le ricerche di vulnerabilità vengono al momento effettuate utilizzando procedure manuali.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni sono configurati per avvenire in automatico. Verificare che ogni postazione abbia attivi gli aggiornamenti automatici del sistema e dei software installati. Ove tecnicamente possibile patch e aggiornamenti dei software vengono schedulati in modo automatico: in caso contrario, tali aggiornamenti vengono eseguiti manualmente da parte del personale incaricato.
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 vi sono dispositivi 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.	Nel caso fossero riscontrati dei problemi, questi saranno risolti attraverso l'installazione di patch o ripristinando il dispositivo. Le vulnerabilità evidenziate tramite le procedure di cui al punto 4.1.1 vengono segnalate ad un supervisore che organizza adeguati gruppi di lavoro per risolverle. Una volta applicate le patch viene richiesta una nuova analisi (punto 4.1.1) e confermata la risoluzione al coordinatore.
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.).	Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione. Garantire che siano state attivate tutte le azioni elencate in questo Vademecum.

					In sede di definizione delle azioni relative alla nuova normativa in materia di tutela dei dati personali verrà formalizzata una analisi dei rischi e delle relative azioni di mitigazione.
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.	Il pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza. Si veda 4.8.1

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.	Si sta procedendo a verificare che l'accesso ai dispositivi da parte degli utenti non avvenga con accessi amministrativi e, ove lo fosse, a convertire l'utenza in una non amministrativa, con accessi di livello più basso. I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD). I privilegi di amministratore sui sistemi server e di sicurezza sono riservati ai responsabili incaricati dell'assistenza, ai tecnici che si occupano della sicurezza. Tali privilegi vengono utilizzati unicamente per lo svolgimento delle attività per le quali essi sono strettamente necessari.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione. I prodotti Axios registrano in automatico ogni accesso effettuato al sistema. Si veda 5.1.1.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Ogni dispositivo avrà una sola utenza amministrativa. Predisporre un elenco degli utenti amministrativi e relativa password assegnata. Tale elenco dovrà essere custodito in cassaforte e messo a disposizione solo al personale addetto alla manutenzione dei dispositivi. Le password dovranno essere non banali e di almeno 14 caratteri di lunghezza. Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. Le utenze amministrative sono in possesso di soggetti nominati in sede di approvazione delle presenti misure minime.

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.	Dopo l'installazione di un nuovo dispositivo sarà cambiata la password di default dell'utente amministratore. È normale e ordinaria pratica tecnica, come tale assicurata dal personale che si occupa delle implementazioni.
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).	Le password utilizzate per le utenze amministrative sono lunghe almeno 14 caratteri e non banali. Vedi azione punto 5.2.1 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 Le credenziali amministrative utilizzate, nei limiti di quanto tecnicamente consentito da ogni dispositivo, vengono scelte in modo da garantire elevati livelli di robustezza.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le password per le utenze amministrative saranno periodicamente aggiornate. Per Axios, vedi parametri indicati nel punto 5.7.1.M Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le password per le utenze amministrative non saranno riutilizzate a breve distanza di tempo. Garantire che le password per le utenze amministrative siano sempre diverse, nella loro successione temporale. Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza. Il sistema di autenticazione è configurato per impedire il riutilizzo delle ultime 6 password per tutti gli utenti.

5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Si assicura che c'è la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori. Garantito se implementata l'azione 5.1.1 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). Gli utenti interni in possesso di credenziali amministrative dei sistemi server e di sicurezza non operano, per attività ordinarie, attraverso tali credenziali. Da parte loro i soggetti esterni non hanno necessità di utilizzo di credenziali ordinarie in quanto intervengono solo per esigenze di tipo manutentivo che richiedano l'utilizzo di credenziali con privilegi elevati.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze amministrative hanno nome utente. Creare in tutte le macchine un utente amministrativo che abbia lo stesso nome utente e sia riconducibile a chi svolge la manutenzione dei dispositivi. In Axios, ad ogni utenza, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi. Ad ogni utenza è attribuito un id, e in particolare le utenze amministrative sono singole e le credenziali sono personali.
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 utenze amministrative anonime saranno utilizzate solo per situazioni di emergenza. Le credenziali amministrative di sistema vengono comunicate e sono utilizzate solo dai tecnici durante gli interventi di gestione dell'infrastruttura.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate in un luogo sicuro. Vedi azione 5.2.1 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. Le credenziali amministrative sono in possesso di personale formalmente incaricato e di provata affidabilità.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano per l'accesso certificati digitali. Non si utilizzano certificati digitali per l'autenticazione.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

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.	Su tutti i dispositivi sono installati sistemi atti a rilevare la presenza e bloccare l'esecuzione di malware e sono aggiornati automaticamente. Vedi azione 2.1.1
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Ogni dispositivo ha attivo un Firewall.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è consentito l'uso di dispositivi esterni nella rete amministrativa. Impedire l'uso di dispositivi non scolastici nella rete amministrativa, per svolgere funzioni amministrative.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Disattivata 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.	Disattivata l'esecuzione automatica dei contenuti dinamici presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Disattivata l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Disattivata 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.	Al momento della connessione di supporti rimovibili sarà eseguita automaticamente una scansione anti-malware.
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.	Viene filtrato il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, attraverso l'impiego di strumenti antispam. Attivare il filtro antispam del programma di gestione della posta elettronica.
8	9	2	M	Filtrare il contenuto del traffico web.	Sarà installato un proxy server che garantisca il filtraggio del contenuto del traffico web. La scuola si dovrà dotare di un Proxy Server in grado di filtrare il traffico web (es. IPCOP, Smoothwall, ZeroShell, ect.) e di alzare il livello di sicurezza senza costi per l'amministrazione.
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).	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa Vedi azione 8.9.2

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.	Sono automatizzate le operazioni sistematiche di back-up su disco di rete (NAS). 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. Vengono eseguite, con schedulazione quotidiana, copie di sicurezza dei dati presenti sui server del fornitore di servizio.
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 disco di rete (NAS) è fisicamente protetto ed è garantita l'accessibilità solo al responsabile della sicurezza informatica e al personale addetto alla manutenzione e all'assistenza tecnica. 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. Le copie dei dati sono conservate con un livello di sicurezza allineato a quello del server principale.
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.	Il disco esterno di conservazione può essere isolato dal sistema semplicemente scollegando il cavo dal server. 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 supporti contenenti le copie vengono ruotati in modo che quelli non in uso non siano accessibili dal sistema informatico

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

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 dispositivi operano in con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall. Vedi azione 8.9.2

IL DIRIGENTE SCOLASTICO

prof.ssa Anna Elisa Barbone

Firmato da:
barbone anna elisa
Motivo:
Dirigente scolastico

Luogo:
Roseto degli Abruzzi
Data: 29/12/2017 23:11:12