Ministero dell'Istruzione dell'Università e Ricerca

II Circolo Didattico "M. Sanseverino" NOLA

DIREZIONE DIDATTICA STATALE 2° CIRCOLO "MARIA SANSEVERINO"NOLA
Via A. Ciccone n°18, 80035 Nola (NA) - cod. fiscale 92019730636 Tel. 081 8234612
www.cdnolasanseverino.it NAEE15300C@istruzione.it naee15300c@pec.istruzione.it

**Protocollo n°3595/B15 del 28/12/2017**

**Misure Minime di Sicurezza ICT per le pubbliche amministrazioni"**

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 | Per le Istituzioni scolastiche l'inventario è regolamentato dal DI 44/2001 e riportato nel modello K del conto patrimoniale. Inoltre viene costantemente aggiornato il registro delle attrezzature informatiche in rete e non. |
| 1 | 3 | 1 | M | Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete. | Gli inventari di cui al punto 1.1.1 vengono aggiornati quando nuove risorse attive vengono collegate 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. | Vedi punti 1.1.1 e 1.3.1<br>Nel laboratorio di informatico, sito al secondo piano della nostra Istituzione scolastica, è presente un sistema di registrazione di dispositivi connessi alla rete e registrazione dell'indirizzo IP. Sistema nominato MIKROTIK. |

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. | Esiste un registro con l'elenco aggiornato dei software installati ed utilizzati dalle postazioni di lavoro presenti negli uffici del Dirigente scolastici, del personale amministrativo, del personale docente facente parte dello STAFF, dei docenti dell'istituto e dei |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | laboratori.<br>Microsoft Windows versione 7/8/10<br>Microsoft office versione 2007/2010/2013<br>Open office versione 4.3<br>Software firewall Mikrotik<br>Controll Class<br>Software per LIM<br>Software per codec video<br>Argo segreteria (Alunni, protocollo e bilancio)<br>Argo registro elettronico (senza accesso ai genitori) |
| 2 | 3 | 1 | M | Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. | Si effettuano verifiche periodiche su tutte le postazioni. |

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. | In tutte le macchine è seguita la seguente procedura:<br>- sono attivati gli aggiornamenti del sistema operativo in modalità automatica<br>-sono attivati firewall locale e dell'antivirus<br>- il backup viene effettuata su unità NAS settimanalmente |
| 3 | 2 | 1 | M | Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione. | Vedi 3.1.1 |
| 3 | 2 | 2 | M | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. | Vedi 3.1.1 |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 3 | 1 | M | Le immagini d'installazione devono essere memorizzate offline. | Le immagini dei sistemi operativi OS Microsoft Windows per la versione 7 sono apposte sulle macchine; per le versioni OS Microsoft Windows 8 e 10 e versioni Microsoft Office 2007/2010/2013 vengono reperite direttamente dall'interno delle macchine tramite software di riconoscimento |
| 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). | Presso la nostra Istituzione scolastica viene eseguita l'assistenza remota tramite i seguenti software: teamviever |

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. | Ad ogni modifica significativa della configurazione viene eseguita la ricerca delle vulnerabilità su tutti i sistemi in rete tramite software antivirus con stampa finale del report rilasciata 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. | Gli antivirus sono attivati su aggiornamento automatico |
| 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 automatizzati limitatamente alle postazione di lavoro. In ambito server (appliance) vengono installate automaticamente solo patch critiche e di sicurezza (security updates) |

| | | | | | |
|---|---|---|---|---|---|
| 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. | Nel laboratorio di informatica, la cui linea ADSL serve tutti i pc dell'area didattica, esiste un firewall MIKROTIK |
| 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. | Attualmente non si sono verificate vulnerabilità non risolte |
| 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.). | Gli unici pc contenenti dati sensibili sono quelli delle postazioni del personale amministrativo il cui software è protetto da ARGO e che sono collegati ad un sistema NAS per le copie di backup chiuso in armadio RAC con chiave |
| 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. | Vedi 4.8.1 e 4.1.1 |

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. | Sulle postazioni di lavoro in uso negli uffici amministrativi e nell'area didattica e nei laboratori sono usati solo da utenti che non hanno privilegi da amministratori di sistema. |
| 5 | 1 | 2 | M | Utilizzare le utenze amministrative solo per effettuare | Vedi punto 5.1.1 |

DIREZIONE DIDATTICA STATALE 2° CIRCOLO "MARIA SANSEVERINO"NOLA
Via A. Ciccone n°18, 80035 Nola (NA) - cod. fiscale 92019730636 Tel. 081 8234612
www.cdnolasanseverino.it NAEE15300C@istruzione.it naee15300c@pec.istruzione.it

| | | | | | |
|---|---|---|---|---|---|
| | | | | 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. | Tutte le utenze dell'area amministrativa e dell'area didattica dotate di password sono gestite dal Dirigente scolastico e dal direttore sei servizi generali ed amministrativi |
| 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. | Ad ogni dispositivo collegato alla rete vengono sostituite le credenziali 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). | Tutte le password rispettano gli standard europei (minimo otto caratteri) |
| 5 | 7 | 3 | M | Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). | Le credenziali delle utenze amministrative vengono sostituite con sufficiente frequenza |
| 5 | 7 | 4 | M | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | Non è possibile utilizzare le stesse password nel breve arco temporale (sei mesi) |
| 5 | 10 | 1 | M | Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. | Gli amministratori di sistema usano due utenze una personale e una di tipo amministrativo che rigorosamente hanno password diverse e di diversa complessità |
| 5 | 10 | 2 | M | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | Le utenze didattiche sono tutte registrate e riconducibili, in termini di responsabilità, ad una sola persona fisica |
| 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 | Solo due utenze amministrative possono essere usate in caso di necessità, e si può risalire a chi le utilizza n quanto sono regolarmente registrate |

| | | | | | |
|---|---|---|---|---|---|
| | | | | uso. | |
| 5 | 11 | 1 | M | Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. | Vedi punti 5.2.1 e 5.10.1 |
| 5 | 11 | 2 | M | Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | Non vengono usati certificati digitali |

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. | Vedi punto 3.1.1 |
| 8 | 1 | 2 | M | Installare su tutti i dispositivi firewall ed IPS personali. | Su tutti i dispositivi è attivato il firewall di Windows |
| 8 | 3 | 1 | M | Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. | Su tutte le macchine è escluso l'utilizzo di dispositivi esterni personali |
| 8 | 7 | 1 | M | Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | Non è attiva l'esecuzione automatica dei contenuti |
| 8 | 7 | 2 | M | Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | Vedi punto 8.7.1 |
| 8 | 7 | 3 | M | Disattivare l'apertura automatica dei messaggi di posta elettronica. | Vedi punto 8.7.1 |
| 8 | 7 | 4 | M | Disattivare l'anteprima automatica dei contenuti dei file. | Vedi punto 8.7.1 |
| 8 | 8 | 1 | M | Eseguire automaticamente una scansione anti-malware dei | Vedi punto 8.3.1 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 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. | La posta istituzionale, in ingresso ed uscita, è gestita dal software Microsoft outlook e dall'antivirus |
| 8 | 9 | 2 | M | Filtrare il contenuto del traffico web. | L'operazione di filtraggio dei contenuti web è effettuata dal firewall MIKROTIK e per gli alunni da Controll Class |
| 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). | Vedi punto 8.9.1 |

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. | Viene effettuato settimanalmente con sistema di protezione dati |
| 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. | Vedi punti 3.3.1 e 4.8.1 |
| 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. | Alla fine di ogni copia di backup il sistema si esclude |

Ministero dell'Istruzione dell'Università e Ricerca

II Circolo Didattico "M. Sanseverino" NOLA

DIREZIONE DIDATTICA STATALE 2° CIRCOLO "MARIA SANSEVERINO"NOLA
Via A. Ciccone n°18, 80035 Nola (NA) - cod. fiscale 92019730636 Tel. 081 8234612
www.cdnolasanseverino.it NAEE15300C@istruzione.it naee15300c@pec.istruzione.it

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 | Vedi punto 10.1.1 |
| 13 | 8 | 1 | M | Bloccare il traffico da e verso url presenti in una blacklist. | Queste funzione è già attiva nel nostro firewall e controll class |

La Dirigente scolastica
Prof.ssa Nicoletta Albano

DIREZIONE DIDATTICA STATALE 2° CIRCOLO DI NOLA (NA)