Andria, 09.01.2018

AL PERSONALE DOCENTE E ATA

Circolare interna n. 53

1. Si informa che, con l'avvio della fase relativa allo scrutinio al termine del primo trimestre dell'anno scolastico corrente, sono già predisposti i Documenti di Valutazione Intermedia di ogni singola studentessa e studente. Al termine delle operazioni di valutazione di ogni corso, saranno resi disponibili on line ad ogni singolo studente a partire dal giorno seguente. I coordinatori delle classi che desiderassero, per ragioni inerenti la didattica, la stampa di qualche documento specifico, sono invitati a rivolgersi alle aa. aa. Altizio e Diasparra in orari che non coincidano con il proprio servizio, per portare a termine le singole operazioni di stampa.

2. Si comunica che viene inviata al personale in servizio la direttiva dello scrivente in materia di politiche di uso corrette delle postazioni informatiche e della rete in istituto, a seguito della emanazione di norme più stringenti intese a limitare l'acquisizione malevola di dati appartenenti alla PA, attraverso introduzioni dirette negli archivi elettronici ovvero indirette mediante codici maligni. L'istituzione scolastica ha già implementato gli accorgimenti tecnici previsti per interdire ovvero limitare le intrusioni di terzi, le quali devono acquisire il rango di ordinarietà nei processi quotidiani negli uffici, nelle classi ed in ogni altro ambiente di apprendimento.

3. Si rammenta al personale interessato nei percorsi di alternanza delle classi III sezioni E ed F e IV sezioni A ed E, che sono confermati gli incontri pomeridiani previsti per il corrente mese dalla convenzione stipulata con il Servizio di Polizia Provinciale e Protezione Civile della Provincia BAT, che qui si riassumono per opportuna memoria:

CLASSI TERZE SEZIONI E ed F

- giovedì 11 gennaio 2018, dalle ore 08:00 alle ore 12:00, incontro a tema su Comunicazioni e Gestione delle Emergenze, con esperti del settore, in Auditorium. Quanto alle modalità, i docenti in servizio all'inizio della prima ora accoglieranno gli studenti nelle rispettive classi e dopo aver annotato eventuali assenze, riporteranno l'evento tra le attività della giornata nel registro elettronico; quindi accompagneranno le classi in auditorium dopo un avviso da parte del personale in servizio. Qui i docenti stazioneranno e si alterneranno come da orario di servizio per vigilare le rispettive classi. Alla conclusione dell'evento i docenti in servizio accompagneranno gli allievi nelle rispettive classi, completando le attività didattiche come da orario di servizio.

CLASSI QUARTE SEZIONI A ed E

- giovedì 11 gennaio 2018, dalle ore 15:00 alle ore 19:00, incontro a tema su Orientamento, sistemi satellitari ed uso di apparati radio, con esperti del settore, in Auditorium. Quanto alle modalità, i docenti tutor presenzieranno alle attività, vigilando gli studenti.

4. Si rende noto che è stato predisposto un modulo unico di adesione alle diverse azioni relative ai PON autorizzati, che risponde a tutte le esigenze di gestione imposte dalla piattaforma ministeriale. Esso, in contemporanea con l'avvio delle singole azioni, verrà personalizzato solo nella parte afferente la loro denominazione. Tutti i tutor, a partire dall'azione in corso, sono invitati ad adoperare il modulo predisposto, disponibile in formato cartaceo presso la a. a. Farinola e inviato in formato elettronico tutti gli interessati.

Si rammenta che tutti gli atti dell'istituzione scolastica sono all'albo www.itescarafa.gov.it e la riproduzione cartacea è presente sul registro predisposto all'ingresso dell'istituzione scolastica.

IL DIRIGENTE
Vito Amatulli

via Bisceglie s.n.c. - 76123 Andria (BT)
Tel. 0883.563636
Fax 0883.563580

www.itescarafa.gov.it
bais05600x@pec.istruzione.it
bais05600x@istruzione.it

Ambito Territoriale Puglia 8
C.M. BAIS05600X
C.F. 90002710722

Protocollo n.0043/M-1 Andria, 08.01.2018

AL PERSONALE DOCENTE E ATA
ALLE STUDENTESSE E AGLI STUDENTI
p.c. Direttore Servizi Generali e Amministrativi, dr.ssa Roberta QUINTO
www.itescarafa.gov.it

DIRETTIVA: MISURE MINIME TUTELA SICUREZZA INFORMATICA IN ISTITUTO – anno scolastico 2017-2018.

IL DIRIGENTE

VISTO il Codice dell'Amministrazione Digitale (CAD) D.lgs. 82/2015, aggiornato e modificato dal D.lgs. 179/2016, attuativo dell'art. 1 della Legge 124 del 7 agosto 2015 di riforma della Pubblica Amministrazione (cd. Legge Madia), recante innovazioni in materia di gestione e conservazione dei dati in formato digitale da parte della Pubblica Amministrazione;

LETTA la Direttiva del Presidente del Consiglio dei Ministri 01.08.15 ove tutte le pubbliche amministrazioni vengono sollecitate a proteggere i sistemi informatici attraverso i quali trattano informazioni e dati in formato digitale quindi a dotarsi di standard minimi di prevenzione e reazione ad eventi cibernetici;

ACQUISITA la circolare 2/2017, con la quale l'Agenzia per l'Italia digitale (AGID) ha indicato alle pubbliche amministrazioni le misure minime necessarie per contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi interni, indicando nella data del 31 dicembre 2017 il termine per l'adempimento;

AMMESSO che Le indicazioni contenute dovranno essere adottate dalle pubbliche amministrazioni entro il 31 dicembre 2017 al fine di fornire tempestivamente un riferimento normativo e consentire di intraprendere percorsi di progressivo adeguamento, secondo quanto già prospettato da AgID e dal CERT–PA sin dall' aprile 2016;

OSSERVATO come la PA necessiti di una adeguata analisi e successivo adeguamento rispetto a quanto stabilito dalla normativa vigente, alla luce anche delle recenti modifiche intervenute in materia di pubblicità e trasparenza di cui al D.lgs. 33/2013, come revisionato a seguito dell'entrata in vigore del d.lgs. 97/2016;

APPRESO che il processo di riforma pone in capo ad ogni PA la necessità di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'Amministrazione, centralizzando in capo ad un ufficio unico il compito di accompagnare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione, con l'obiettivo generale di realizzare una amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

PREVISTO che le misure sono parte integrante del più ampio disegno delle regole tecniche per la sicurezza informatica della Pubblica Amministrazione, in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici;

AVVERTITA la necessità di dotarsi di standard minimi di prevenzione e reazione e rendere costanti i processi di manutenzione e aggiornamento della propria infrastruttura informatica interna;

INDICATO nella figura del Dirigente pro tempore, prof. Vito Amatulli, la figura del Responsabile alla Transizione Digitale, nel rispetto di quanto riportato all'Art. 17 del Codice dell'Amministrazione Digitale vigente, il quale assume contestualmente l'onere di seguire la transizione verso un'amministrazione digitale ed aperta, garantendo gli adempimenti conseguenti;

PREVISTI che al Dirigente sono attribuiti compiti di coordinamento e di impulso ai processi informatici, evidenziati in sintesi come segue:

a) Coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare la coerenza con gli standard tecnici e organizzativi comuni;

b) Indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, fomiti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c) Indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'art. 51, comma 1;

d) Accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità, attuando quanto già previsto dalla L. 09.01.04, n. 4;

e) Analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) Cooperazione alla revisione ed alla azione di riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

g) Indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo, gestione e controllo dei sistemi informativi di telecomunicazione e fonia anche di terzi;

h) Progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) Promozione delle iniziative attinenti l'attuazione delle direttive impartite da norme nazionali.

STABILISCE LE SEGUENTI REGOLE DI COMPORTAMENTO, IN RELAZIONE ALL'USO INDIVIDUALE OVVERO COLLETTIVO DELLE STRUMENTAZIONI ELETTRONICHE ED INFORMATICHE PRESENTI E FUNZIONANTI IN ISTITUTO, NOMENCLATE COME SEGUE:

1. E' stato implementato un archivio delle risorse attive, qualificandole individualmente e attraverso l'analisi del loro traffico: pertanto, ogni dispositivo sarà tracciato.
2. L'archivio sarà aggiornato automaticamente con l'accesso alla rete di nuovi dispositivi approvati e riconosciuti, quindi anch'essi tracciabili.

3. L'archivio sarà gestito attraverso l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando l'indirizzo di ognuno.
4. Il sistema di accesso alla rete consente sia l'individuazione dei singoli dispositivi e sia la registrazione telematica della loro autorizzazione di accesso.
5. E' presente un archivio di applicativi con le relative versioni, necessarie per ciascun tipo di sistema, compreso il server – stazioni di lavoro – portatili – *tablet* - che sono autorizzati all'installazione. Pertanto, l'installazione di applicativi proprietari di cui l'istituto scolastico non disponga di licenza è assolutamente vietato. Al fine del rispetto sostanziale del punto in esame, saranno eseguite periodicamente scansioni su tutti i sistemi, volte a rilevare e rimuovere la presenza di applicativi non autorizzati, senza alcun preavviso.
6. Gli assistenti tecnici utilizzeranno configurazioni di sistema sicure di tipo standard, consigliate dallo stesso produttore, per proteggere i sistemi operativi. Tali configurazioni di tipo standard saranno impiegate su tutte le tipologie di sistemi adoperati dall'istituzione scolastica. Ne consegue che, in presenza di eventuali compromissioni nella funzionalità, sarà attuato il ripristino adoperando la configurazione standard. Si precisa che le immagini delle installazioni sono memorizzate offline.
7. Gli assistenti tecnici eseguono tutte le operazioni di amministrazione remota di server, stazioni di lavoro, dispositivi connessi alla rete e apparecchiature analoghe per mezzo di connessioni protette.
8. Gli assistenti tecnici, a seguito di ogni modifica significativa nella configurazione dei sistemi, eseguono la ricerca delle vulnerabilità sia dei singoli elaboratori in rete ricorrendo a strumenti automatici che restituiscano alla risorsa umana individuata in qualità di Amministratore di Sistema un rapporto delle criticità eventualmente riscontrate. Gli strumenti di scansione delle vulnerabilità sono usati regolarmente e aggiornati e pertanto non devono essere manomessi ovvero disattivati per nessuna ragione. Tutti i rischi devono essere tempestivamente e radicalmente rimossi.
9. Saranno installati sui sistemi connessi alla rete locale, programmi utili a rilevare la presenza e bloccare l'esecuzione di script malevoli. Essi saranno anche mantenuti aggiornati anche in modalità automatica.
10. Il firewall dell'istituto è gestito con un applicativo aggiornato regolarmente.
11. La pratica di aggiornamento dei sistemi operativi e delle applicazioni deve essere eseguita automaticamente ovvero differita per ragioni di tempo ma sempre realizzata.
12. I privilegi di amministratore sono limitati ai soli assistenti tecnici i quali, in accordo con il Dirigente, valuteranno le necessità di operare una modificazione della configurazione dei sistemi operativi interessati. Per lo scopo, è stato attuato il sistema del doppio login su ogni elaboratore.
13. Viene mantenuto l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata dall'Amministratore di Sistema, sentito il parere obbligatorio e vincolante del Dirigente. Ogni nuovo dispositivo collegato alla rete deve essere censito dall'Amministratore di Rete. Viene vietato l'uso di dispositivi esterni non necessari alle attività didattiche.
14. Il Custode delle PW è invitato, quando l'autenticazione a più fattori non sia supportata, a far usare per le utenze amministrative credenziali di elevata robustezza (cioè con almeno 14 caratteri), impedendo ed ammonendo preventivamente all'uso di credenziali deboli. Il Custode delle PW assicurerà che le credenziali delle utenze amministrative vengano sostituite con una frequenza almeno trimestrale ed impedirà che credenziali

già usate possano essere riutilizzate a breve. Tutte le credenziali ammnistrative saranno custodite dal Dirigente nella propria cassaforte, per garantirne disponibilità e riservatezza.

15. L'Amministratore di Rete curerà affinché tutte le utenze siano nominative e riconducibili ad una sola persona; il ricorso ad utenze anonime deve avvenire solo in presenza di situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne abbia fatto uso.
16. Quale politica di uso corretto della rete, tutti coloro i quali accedono a postazioni connesse devono disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili; devono disattivare l'esecuzione automatica dei contenuti dinamici (ad es. macro) presenti nei file; devono disattivare l'apertura automatica dei messaggi di posta elettronica; devono disattivare l'anteprima automatica dei contenuti dei file; devono filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario; devono filtrare il contenuto del traffico via web; bloccare il traffico da e verso url presenti in una lista nera; evitare di usare archivi rimuovibili (ad es. chiavette usb), in particolare negli uffici di segreteria. I questa circostanza, i file dovranno essere inviati per posta elettronica, adoperando le postazioni libere (ma tracciate) in istituto, anche in tempo reale.
17. Quale politica di uso corretto della rete, l'Amministratore di Rete effettua con cadenza almeno settimanale una copia di sicurezza dei dati residui presenti, utili a ripristinare il sistema in caso di anomalie. La riservatezza delle informazioni contenute nelle copie di sicurezza avviene proteggendo fisicamente il supporto nella cassaforte del Dirigente.
18. Le prescrizioni che precedono sono portate a conoscenza di tutto il personale in servizio e affisse in tutti gli ambienti collettivi scolastici, perché anche le studentesse e gli studenti ne abbiano cognizione.
19. Le prescrizioni che precedono sono dettate dall'amministrazione centrale per adeguare ogni unità periferica ai percorsi comuni vocati alla corretta digitalizzazione che prevede un naturale percorso di costante adeguamento sia alla utilità delle risorse disponibili sia ai pericoli intrinseci nella loro gestione poco attenta.
20. In considerazione dei danni che potrebbero verificarsi alla rete LAN interna a causa di un uso improprio dei sistemi collegati alla rete e grazie alla presenza dei sistemi di tracciamento automatico, si precisa che eventuali anomalie saranno immediatamente localizzabili.

IL DIRIGENTE
prof. Vito Amatulli
firma autografa omessa
sostituita a mezzo stampa
art. 3 co. 2 D.lgs. 39/93