1°CD GIUGLIANO
P.zza Gramsci, 7 - 80014
Giugliano in Campania (NA)
tel.\fax 081 895 13 00
e-mail - naee139006@istruzione.it
- naee139006@pec.istruzione.it
www.primocircolodidattico.edu.it
cod.fisc. 80101750638

A tutto il personale Interno della Scuola

OGGETTO: Avviso al personale interno della scuola per l'affidamento dell'incarico di Amministratore di Sistema ai sensi del provvedimento del Garante della Privacy del 27 Novembre 2008 (G.U. n° 300 del 24 dicembre 2008)"Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" rivolto al personale interno della scuola.

IL DIRIGENTE SCOLASTICO del Primo Circolo Didattico Dott.ssa Olimpia Finizio in qualità di Titolare del Trattamento dei dati ai sensi del Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679)

VISTO l' art. 28 del Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679);

CONSIDERATO che i Titolari sono tenuti , ad adottare misure di sicurezza "idonee e preventive in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile;

CONSIDERATO inoltre che il Titolare è tenuto ad individuare solo soggetti che per esperienza , capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza;

CONSTATO che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza , costituendo una delle scelte fondamentali che, unitamente a quella relativa alle tecnologie, contribuiscono ad incrementare la complessiva sicurezza dei trattamenti svolti e che pertanto la valutazione delle caratteristiche soggettive e l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e rammentando che vi sono alcuni reati previsti dal codice penale per il quale rivestire le funzioni di amministratore di sistema costituisce una circostanza aggravante (abuso della qualità di operatore di sistema nell'accesso abusivo a sistema informatico o telematico — art. 615 ter c.p. — 0 di frode informatica — art. 640 ter c.p.- oppure per le fattispecie di danneggiamento di informazioni, dati e programmi informatici artt. 635 bis e ter c.p. — e di danneggiamento di sistemi informatici e telematici — artt. 635-quater e quinques).

RENDE NOTO

che intende procedere all'affidamento dell'incarico di Amministratore di Sistema come previsto dal provvedimento del Garante della Privacy del 27/11/2008 (G.U. n°300 del 24/12/2008) così come modificato dal Provvedimento del Garante della Privacy del 25/06/2009 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", prioritariamente al personale interno alla scuola.

L'importo per tale incarico sarà pari ad € 1.500,00 (millecinquecento/00) omnicomprensivo di ogni contributo e ritenuta – Lordo Stato -

Tale nomina è in relazione alla gestione del sistema informatizzato della scuola e in particolare per:

- Assicurare la gestione delle prime credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso, se necessario
- Verificare periodicamente la funzionalità delle copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- Verificare periodicamente la funzionalità delle altre disposizioni di sicurezza (antivirus, firewall, screen saver) e il loro stato di aggiornamento;
- Operare da interfaccia tecnica nei riguardi degli incaricati del Responsabile esterno del trattamento addetti alla manutenzione e alla gestione dei sistemi informatici, se richiesto dal **Titolare** e/o dal **DSGA**;
- Operare da interfaccia tecnica con il Responsabile esterno del Trattamento per tutto ciò che riguarda i sistemi informatici, se richiesto dal **Titolare** e/o dal **DSGA**;
- Effettuare il primo intervento di messa in sicurezza del sistema informatico in caso di data breach o di crash funzionale;
- Effettuare quanto altro predisposto come attività e responsabilità nelle procedure dell'Istituto per la gestione e il controllo del sistema informativo e delle disposizioni di sicurezza informatica.

L'oggetto dell'incarico è di sotto riportato:

- Implementare un inventario delle risorse attive;
- Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete;
- Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP;
- 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;
- Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato;
- Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi;
- Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione;
- Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard;
- Le immagini d'installazione devono essere memorizzate offline;
- 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);
- 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;
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza;
- Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni;
- Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli

air-gapped, adottando misure adeguate al loro livello di criticità;
- 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;
- 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.);
- 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;
- Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi;
- Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato;
- Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata;
- Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso;
- Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri);
- Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging);
- Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history);
- Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse;
- Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona;
- 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;
- Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
- Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette;
- 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;
- Installare su tutti i dispositivi firewall ed IPS personali;
- Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali;
- Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili;
- Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file;
- Disattivare l'apertura automatica dei messaggi di posta elettronica;
- Disattivare l'anteprima automatica dei contenuti dei file;
- Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione;
- Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam;
- Filtrare il contenuto del traffico web;
- 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);
- Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema;
- 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;
- 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;
- 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;
- Bloccare il traffico da e verso url presenti in una blacklist.

L'attività dovrà essere svolta attenendosi alle seguenti modalità generali:

- Operando alle dipendenze del Titolare del trattamento dei dati ed eseguendo puntualmente le istruzioni impartite dallo stesso;
- Rispettando durante le attività svolte le misure di sicurezza previste dalla legge e specificate nel Registro del trattamento dei dati e nelle procedure specifiche;
- Garantendo la massima riservatezza nel trattamento dei dati;
- Informando tempestivamente il Responsabile del trattamento di anomalie nel funzionamento del sistema informatico che possano pregiudicare il corretto trattamento dei dati.

In particolare l'Amministratore di sistema avrà l'obbligo:

a) di rispettare il segreto sulle informazioni e sui dati personali di cui viene a conoscenza nell'esercizio delle proprie funzioni (art.326 del codice Penale e art.15 del DPR 13/1957). Tale obbligo permarrà anche dopo la cessazione dell'incarico;

b) di conoscere e di impegnarsi a rispettare, sotto la propria personale responsabilità, quanto indicato nell'allegato b del "Disciplinare tecnico in materia di misure minime di sicurezza" trattare i dati personali solo se indispensabile in relazione all'assolvimento degli incarichi assegnati;

c) del rispetto dei requisiti di diligenza professionale, richiesti dall'articolo 2050 del codice civile;

d) dell'adeguamento preventivo dell'adozione ai contenuti espressi a quanto riportato nella Circolare 18 aprile 2017, n. 2/2017 della AGENZIA PER L'ITALIA DIGITALE, «Misure Minime di sicurezza ICT per le pubbliche amministrazioni», ripreso da «MIUR.AOODGCASIS.REGISTRO UFFICIALE(U).0003015.20-12-2017.

L'incarico avrà la durata di un anno a decorrere dalla data di stipula del contratto.

Il compenso sarà liquidato previa verifica dell'operato dell'incaricato da parte del Titolare e del

Responsabile del Trattamento. Possono presentare domanda figure professionali in possesso

dei seguenti requisiti;

- Titolo di studio adeguato (Diploma di laurea in Informatica, Ingegneria o di perito informatico, elettronico, elettrotecnico);

- Documentata esperienza nello svolgimento delle mansioni di Amministratore di sistema presso pubbliche amministrazioni;

- Documentata esperienza, di attività nell'ambito della applicazione del Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679);

Gli aspiranti dovranno fare pervenire domanda in busta chiusa con dicitura contiene " Candidatura per incarico quale amm.re di sistema" , improrogabilmente entro le ore 12,00 del giorno 21/05/2020 (a pena di esclusione). Non farà fede il timbro di spedizione, ma quello di arrivo presso l'Ufficio Postale di destinazione indirizzata al Dirigente Scolastico dell'Istituto presso Piazza Gramsci 7, a mezzo di raccomandata a/r oppure a mezzo pec all'indirizzo naee139006@pec.istruzione.it

La Busta di cui sopra dovrà contenere al suo interno la domanda in carta semplice e le dichiarazioni

dei titoli posseduti. Alla domanda dovrà essere allegata la seguente documentazione:

- il curriculum vitae in formato europeo, firmato in ogni pagina dal quale risulti il possesso dei requisiti culturali e professionali richiesti, nonché di tutti i titoli validi secondo i parametri di affidamento sopra riportati;

La mancata e/o incompleta presentazione della domanda, della documentazione e delle dichiarazioni innanzi indicate, nonché l'inosservanza dei termini e delle prescrizioni contenute nel presente Avviso di selezione pubblica, saranno considerate cause di esclusione dal procedimento.

I criteri per l'affidamento dell'incarico sono i seguenti:

TITOLI	PUNTI MAX
DIPLOMA DI PERITO INFORMATICO,ELETTRONICO,ELETTROTECNICO	10
DIPLOMA DI LAUREA IN INFORMATICA ,INGEGNERIA O DISCIPLINE EQUIPOLLENTI	20
SPECIALIZZAZIONE UNIVERSITARIA O MASTER ATTINENTI	5
ECDL AVANZATA, ATTESTATI INFORMATICI DI ALMENO 60 ORE E EIPASS(4 valutabili)	5 Punti per ciascun attestato MAX 20
INCARICHI DI AMMINISTRATORE DI SISTEMA PRESSO ISTITUZIONE SCOLASTICHE STATALI (5 anni valutabili)	6 Punti per ogni anno scolastico MAX 30
INCARICHI DI AMMINISTRATORE DI SISTEMA PRESSO ALTRE PUBBLICHE AMMINISTRAZIONI(5 anni valutabili)	3 Punti per ogni anno solare MAX 15
totale	**100**

A parità di punteggio sarà considerata la candidature del più giovane di età.

Qualora il servizio non risponda a criteri di efficacia e tempestività l'Amministrazione può revocare l'incarico, dandone comunicazione all'interessato con 15 giorni di preavviso.

L'Istituzione si riserva la facoltà, a proprio insindacabile giudizio, di differire, spostare, revocare, modificare

il presente procedimento di selezione o di non affidare l’incarico in oggetto, senza alcun diritto dei concorrenti a rimborso spese o quant'altro.

Non saranno presi in considerazione i plichi che, per qualsiasi causa o motivo, perverranno oltre il termine stabilito all’ Ufficio di Segreteria della scuola.

L'apertura delle buste contenenti le offerte sarà effettuata da una opposita commissione formata da tre componenti il giorno 22/05/2020 alle ore 10,00. Alla operazione predetta potrà presenziare il diretto interessato oppure un delegato munito di specifica delega.

Per ogni informazione in merito, gli interessati possono rivolgersi al Direttore dei Servizi Generali

ed Amministrativi. Il presente avviso viene pubblicato all’Albo e sul sito web dell'Istituto.

IL DIRIGENTE SCOLASTICO

Dott.ssa Olimpia FINIZIO