I.C. - "G. RODARI - G. NOSENGO"-GRAVINA DI CATANIA
Prot. 0008585 del 22/12/2017
B-15 (Uscita)

REPUBBLICA ITALIANA - REGIONE SICILIA
MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
ISTITUTO COMPRENSIVO STATALE "G. RODARI-G.NOSENGO"
VIA SAN PAOLO N. 107 - CAP 95030 - GRAVINA DI CATANIA (CT)
Distretto 18° - Cod. Mecc. CTIC8A4007 - C.F. 93190610878 - TEL - FAX 095/7258150
e-mail ctic8a4007@istruzione.it – ctic8a4007@pec.istruzione.it
www.icrodarinosengo.gov.it

Al Sito WEB

Al personale incaricato della manutenzione dei sistemi informatici
PC e server
Ditta Sfera S.r.l.- Catania
sferainnovazione@pec.it

e, p.c.,

Responsabile della Transizione Digitale
Sig.ra Angela Epifania Spampinato

Ditta NetSense S.r.l.
netsense@pec.it

OGGETTO: INDICAZIONI OPERATIVE PER IL MANTENIMENTO DELLE MISURE DI SICUREZZA MINIME NEI SISTEMI ICT.

IL DIRIGENTE SCOLASTICO

VISTO il Codice dell'Amministrazione Digitale (CAD) di cui al D.lgs. 82/2005, come modificato dal D.lgs. 179/2016, attuativo dell'art. 1 della Legge 124/2014 di riforma della Pubblica Amministrazione (cd. Legge Madia);

CONSIDERATO CHE le modifiche apportate al Codice dell'Amministrazione digitale dal D.lgs. 179/2016 sono finalizzate a rendere finalmente attuabile la transizione alla modalità operativa digitale e ad indirizzare i processi di riorganizzazione finalizzati alla realizzazione di un'Amministrazione digitale e aperta,

di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

VISTA la nomina del "Responsabile della transizione digitale", giusto prot. 8547 del 21.12.2017,

PRESO ATTO CHE i processi e i procedimenti attivi in Istituto necessitano di una adeguata analisi e del 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 cd. Freedom of Information Act (FOIA);

VISTO quanto disposto dal DPCM 01 Agosto 2015 in termini di misure di sicurezza ICT minime;

PRESO ATTO CHE per quanto sopra, i sistemi informatici dispiegati in Istituto dovranno essere modificati ed allineati a quanto risultato da una prima analisi dei processi;

RILEVATO CHE alla Ditta Sfera S.r.l. di Catania è affidato il compito della manutenzione dei PC e dei server dell'Istituto;

VISTA l'acquisizione del servizio annuale NET-SECURITY, giusto prot. n. 8208/B15 del 06.12.2017, per l'adozione delle misure minime di sicurezza relative alla rete dati dell'Istituto;

DETERMINA

che la Ditta Sfera S.r.l.- Catania effettui con regolarità i prescritti indicati nel seguito.

A) Attività da effettuare con regolarità su PC e Server

1. Scaricare il programma free **CCleaner** (https://ccleaner.it.softonic.com) e:
   a. installarlo su tutti i PC dell'Istituto dotati di SO Windows;
   b. effettuare una scansione confrontando i programmi esistenti nel PC con quelli della lista di seguito riportata;
   c. aggiornare la lista se un software non fosse presente o, al contrario, disinstallare eventuale software non riconosciuto e non presente nella lista.
   d. Ripetere ogni sei mesi la verifica.

NET 4.7.1,	7-Zip,	Activ Inspire,	Adobe Air,
Adobe Flash	Dropbox,	Italc,	Microsoft Office Power

Player,			Point,
Adobe Reader,	Elite Panaboard,	Java 8,	Microsoft Office Word,
Avira	EyeBoard,	Java JDK,	Microsoft Outlook,
CCleaner,	Genius Board,	K-Lite Codec,	Mozilla Firefox,
Classflow,	Geogebra,	LibreOffice Calc,	Mozilla Thunderbird,
Classic Start,	GIMP,	LibreOffice Draw,	OneDrive,
Deep Freeze,	Google Chrome,	LibreOffice Impress,	Opera,
Drive Vaccine,	Google Dive,	LibreOffice Math,	Oxford Dictionary,
Metasploit	ImgBurn,	LibreOffice Writer,	PDF Creator,
Cobian Backup	AVG Free	Malwarebytes,	Shockwave,
Skype,	Windows Defender,	Microsoft Office Excel,	Silverlight,
Team Viewer,	WinRAR,	VLC,	AVG Free
Hardentools	(*)	(*)	(*)

(*) la lista è da mantenere aggiornata e da completare con software ad uso didattico (LIM, ecc.)

2. Scaricare il programma free **hardentools** (https://github.com/securitywithoutborders/hardentools/releases) e:
    a. installarlo su tutti i PC dell'Istituto dotati di SO Windows;
    b. effettuare una scansione eliminando:
        i. - esecuzione di VBScript and Javascript
        ii. - esecuzione di autorun e autoplay
        iii. - esecuzione di powershell
        iv. - estensione di file utilizzati principalmente a scopi malevoli
        v. - esecuzione di Macro Office

vi. - esecuzione di oggetti OLE
vii. - esecuzione activeX
viii. - esecuzione Javascript in documenti PDF
ix. - esecuzione di oggetti embedded in documenti PDF

c. ripetere ogni sei mesi la verifica.

3. Scaricare il programma free **Metasploit** (https://windows.metasploit.com/metasploitframework-latest.msi) e:
   a. installarlo in un PC dell'Istituto dotato di SO Windows e connesso in rete;
   b. installarne i demoni i ogni PC della rete dotato di SO Windows;
   c. effettuare una scansione della rete con i PC accesi, per verificare i livelli di vulnerabilità di ciascuno di essi.
   d. Ripetere ogni sei mesi la verifica.

4. Dare disposizioni al personale incaricato affinché in ogni PC e server di Istituto, dotati di SO Windows, si:
   a. configuri un account utente con privilegi di amministratore;
   b. imposti una password di amministratore;
   c. sigillare in busta chiusa la password di amministratore e consegnarla al Dirigente;
   d. impostare i privilegi dell'account utente in uso sul PC a "User".

5. Scaricare il programma antivirus free **AVGFree** (https://www.avg.com/it-it/free-antivirus-download) e:
   a. installarlo su tutti i PC dell'Istituto dotati di SO Windows;
   b. attivarne gli aggiornamenti automatici;
   c. effettuare una scansione eliminando le minacce attive.
   d. Ripetere ogni sei mesi la verifica, mantenendo aggiornato il software.

6. Attivare, in ogni PC dell'Istituto dotato di SO Windows, il firewall di Windows.

7. Scaricare il programma antivirus free **Cobian Backup** (http://www.cobiansoft.com/index.htm) e:
   a. installarlo su tutti i PC della segreteria dotati di SO Windows;
   b. attivare il backup automatico almeno delle cartelle Documenti e Desktop di ogni utente attivo verso cartelle condivise da NAS o Server in rete.
   c. Mantenere aggiornato il software.

B) Attività da effettuare sulla rete dati

Collaborare con il personale della Ditta fornitrice dell'Apparato Net-Security per la messa in sicurezza e l'attivazione delle anagrafiche dei sistemi in rete previste dalle misure minime. La responsabilità delle implementazioni delle misure sulla rete dati resta in capo all'azienda fornitrice del servizio, la quale a sua volta è chiamata a pronta collaborazione con il Responsabile della Transizione Digitale.

C) Collaborazione con il Responsabile della transizione digitale

La continua collaborazione è volta ad aggiornare costantemente il Modulo di Implementazione delle misure minime di sicurezza ICT alla luce di modifiche o aggiornamenti dei sistemi informativi e della normativa vigente.

Il Dirigente Scolastico
Dott.ssa Anna Maria Sampognaro

Documento firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate e sostituisce il documento cartaceo e la firma autografa