N. 8 del Reg. Delib.

Prot. N._____

C O M U N E D I M E L A R A

Provincia di Rovigo

COPIA DEL VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: Approvazione misure minime di sicurezza ICT per le pubbliche amministrazioni (MMS-PA) ex circolare della Agenzia per l'Italia Digitale n. 2 del 18 aprile 2017.

L'anno duemilaventi addì ventitre del mese di gennaio ore 15:30 nella sede del Comune di Melara si è oggi riunita la Giunta Municipale nelle persone dei Sigg.ri:

MARCHESINI ANNA	SINDACO	Presente
BARALDI ADOLFO	VICESINDACO	Assente
GUERZONI LORENZO	ASSESSORE	Presente

Partecipa con funzioni consultive, referenti, di assistenza e verbalizzazione (art. 97 c. 4° D.Lgs. 267/2000) il Segretario comunale: Dr. Gino Prandini.

Il Sindaco, constatato che gli intervenuti sono in numero legale dichiara aperta la riunione ed invita a deliberare sull'oggetto sopra indicato.

LA GIUNTA COMUNALE

PREMESSO CHE:

• gli attacchi informatici ai sistemi rappresentano oggi un elemento di grande criticità per le aziende private e le pubbliche amministrazioni;

• l'attenzione del legislatore e del governo nazionale ed europeo è volta ad attività di prevenzione e difesa rispetto agli attacchi informatici e più in generale a favorire le azioni di ICT Security delle Pubbliche Amministrazioni;

• in questo contesto sono stati emanati vari provvedimenti legislativi quali il DPCM del 24 Gennaio 2013 recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", il DPCM 27 gennaio 2014 che approva il "quadro strategico nazionale per la sicurezza dello spazio cibernetico" e la direttiva 1 agosto 2015 della Presidenza del Consiglio "Sistema di informazione per la sicurezza della Repubblica";

DATO ATTO altresì che l'art. 14 -bis del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera a) , tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica;

RICHIAMATA a tal fine la direttiva del 1° agosto 2015 del Presidente del Consiglio dei Ministri che ha imposto l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte;

VISTA e richiamata la circolare della AGENZIA PER L'ITALIA DIGITALE n. 2 del 18 aprile 2017, rubricata "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»." (la presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella Gazzetta Ufficiale n. 79 del 4 aprile 2017) con cui sono introdotti l'insieme dei controlli che costituiscono le Misure Minime AgID, denominati AgID Basic Security Controls (ABSC) partendo dalla base, già consolidata e assai apprezzata dalla comunità mondiale degli esperti di sicurezza, costituita dai cosiddetti "SANS 20" (oggi noti come Critical Security Controls) emessi dal SANS Institute;

DATO ATTO:

• che al fine da non costringere le Amministrazioni, soprattutto quelle più piccole, ad introdurre misure esagerate per la propria organizzazione, con evidente inutile dispendio di risorse, i singoli controlli CSC sono stati trasposti nei controlli ABSC suddividendoli in famiglie di misure di dettaglio più fine, che possono essere adottate in modo indipendente proprio per consentire alle Amministrazioni di graduare il proprio sistema di sicurezza per meglio adattarlo alle effettive esigenze della specifica realtà locale;

• che per facilitarne ulteriormente l'adozione, minimizzando gli impatti implementativi sull'organizzazione interessata, i controlli sono inoltre stati suddivisi in tre gruppi verticali, riferiti a livelli complessivi di sicurezza crescente. I controlli del primo gruppo (livello "Minimo") sono quelli strettamente obbligatori ai quali ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve

essere conforme in termini tecnologici, organizzativi e procedurali: essi dunque rappresentano complessivamente il livello sotto al quale nessuna Amministrazione può scendere;

• che i controlli del secondo gruppo (livello "Standard") rappresentano la base di riferimento per la maggior parte delle Amministrazioni, e costituiscono un ragionevole compromesso fra efficacia delle misure preventive ed onerosità della loro implementazione;

• che i controlli del terzo gruppo (livello "Alto") rappresentano infine il livello adeguato per le organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati, ma anche l'obiettivo ideale cui tutte le altre organizzazioni dovrebbero tendere.

PRESO ATTO che ogni Amministrazione dovrà pertanto avere cura di individuare al suo interno gli eventuali sottoinsiemi tecnici e/o organizzativi, caratterizzati da una sostanziale omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi;

PRECISATO che per quanto riguarda i contenuti, le Misure Minime prevedono, nella loro formulazione attuale, otto insiemi (o "classi") di controlli così dettagliati:

- I controlli delle prime due classi (ABSC 1 e 2) riguardano rispettivamente l'inventario dei dispositivi autorizzati e non autorizzati e quello dei software autorizzati e non autorizzati. In pratica essi impongono all'organizzazione di gestire attivamente i dispositivi hardware e i pacchetti software in uso, predisponendo e mantenendo aggiornati, a diversi livelli di dettaglio e con differenti modalità attuative a seconda del livello di sicurezza, i rispettivi inventari, e prevedendo inoltre meccanismi per individuare e/o impedire tutte le anomalie operative, ossia l'impiego di elementi non noti e/o esplicitamente autorizzati.

- I controlli della terza classe (ABSC 3) riguardano la protezione delle configurazioni hardware e software sui sistemi in uso presso l'organizzazione.

- I controlli della quarta classe (ABSC 4) sono finalizzati ad individuare tempestivamente, e correggere, le vulnerabilità dei sistemi in uso, minimizzando la finestra temporale nella quale le vulnerabilità presenti possono essere sfruttate per condurre attacchi contro l'organizzazione.

- I controlli della quinta classe (ABSC 5) sono rivolti alla gestione degli utenti, in particolare gli amministratori, ed hanno lo scopo di assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi sui sistemi in uso.

- I controlli della sesta classe (ABSC 8) hanno lo scopo di contrastare l'ingresso e la diffusione nell'organizzazione di codice malevolo di qualsiasi provenienza.

- I controlli della settima classe (ABSC 10) sono relativi alla gestione delle copie di sicurezza delle informazioni critiche dell'organizzazione, che in ultima analisi sono l'unico strumento che garantisce il ripristino dopo un incidente.

- L'ottava ed ultima classe (ABSC 13) riguarda infine la protezione contro l'esfiltrazione dei dati dell'organizzazione, in considerazione del fatto che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

PRESO ATTO pertanto che, come previsto dalla citata circolare, ciascuna Amministrazione debba non solo implementare i controlli rilevanti, ma anche dare brevemente conto della modalità di implementazione compilando un apposito modulo il quale andrà poi firmato digitalmente/ marcato temporalmente e conservato

dall'Amministrazione stessa, salvo inviarlo al CERT-PA in caso di incidenti e che detto adempimento debba avvenire entro il 31 dicembre 2017 comunque in una logica evolutiva e/o di convergenza;

VISTO inoltre il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679) - pienamente applicato entro il 25 maggio 2018 - con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea aumentando il livello di responsabilizzazione introducendo il concetto di misure idonee alle organizzazioni che sono chiamate ad attuare quanto necessario per la sicurezza a fronte di pesanti sanzioni;

DATO ATTO che l'aspetto primario per un adeguato piano di sicurezza è quello organizzativo, questa giunta intende definire con le presenti linee guida gli aspetti fondamentali in relazione alle responsabilità, individuazione dei dati da difendere, formazione agli utenti, principali misure tecniche;

VISTO l'allegato modulo di implementazione di cui all'allegato 2 della CIRCOLARE 18 aprile 2017 , n. 2/2017 emanata dalla Agenzia per l'Italia Digitale, debitamente compilato nei controlli del primo gruppo (livello "Minimo") ovvero quelli strettamente obbligatori ai quali ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, che deve essere conforme in termini tecnologici, organizzativi e procedurali rappresentando complessivamente il livello sotto al quale nessuna Amministrazione può scendere, denominato Modulo di implementazione delle Misure Minime di Sicurezza ICT per le pubbliche amministrazioni (MMS-PA), sottoscritto digitalmente dal competente Responsabile di Area e con marcatura temporale, parte integrante e sostanziale del presente atto (allegato A);

ACQUISITO ed allegato il solo parere di regolarità tecnica espresso dal competente responsabile dell'Area, ai sensi dell'art.49, comma 1, del D.Lgs. n.267/2000, considerato che l'atto non necessita di parere di regolarità contabile in quanto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente;

Con voti favorevoli, unanimi, resi nei modi di legge;

DELIBERA

Per le motivazioni esposte in premessa e che qui si intendono interamente richiamate:

1. di approvare il Modulo contenente le Misure Minime di Sicurezza ICT per le pubbliche amministrazioni (MMS-PA) debitamente compilato nei controlli del primo gruppo (livello "Minimo"), nel testo allegato al presente provvedimento quale parte integrante sostanziale (allegato A) firmato digitalmente con marcatura temporale, conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso;

2. di dare mandato al Responsabile dei sistemi informativi dell'Ente di attuare le misure MMSPA individuate e di portarle a conoscenza per quanto necessario ai responsabili di Area e Settore dell'Ente.

3. di incaricare il competente responsabile del settore di effettuare le verifiche del caso circa l'obbligo di pubblicazione previsto dal D. Lgs. 14/03/2013 n° 33 e s.m.i.;

4. di dichiarare altresì il presente atto, con separata unanime votazione, immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs. 18/08/2000, n.267 stante la necessità di procedere entro la scadenza di legge.

COMUNE DI MELARA

Provincia di Rovigo

****

SERVIZIO PROPONENTE: AMMINISTRATIVO

Il sottoscritto responsabile del servizio, interpellato ai sensi dell'art. 49 del d. lgs. 267/2000 circa la **Regolarita' tecnica** dell'assumenda delibera avente ad oggetto "Approvazione misure minime di sicurezza ICT per le pubbliche amministrazioni (MMS-PA) ex circolare della Agenzia per l'Italia Digitale n. 2 del 18 aprile 2017." esprime parere: Favorevole

Data: 22-01-2020

f.to Il Responsabile del servizio
ISABELLA FAVALLI
Sottoscritto digitalmente ai sensi dell'art. 21
D.Lgs. N. 82/2005 e ss.mm.

Il presente verbale viene sottoscritto come segue:

f.to Il Sindaco
ANNA MARCHESINI

f.to Il Segretario
Dr. Gino Prandini

REFERTO DI PUBBLICAZIONE (art. 124 D.Lgs. 267/2000)

Certifico, io sottoscritto Segretario, su conforme dichiarazione del messo che copia del presente verbale viene pubblicato il giorno _____ all'albo pretorio ove rimarrà esposto per 15 giorni consecutivi.

f.to Il Segretario
Dr. Gino Prandini

TRASMISSIONE AI CAPIGRUPPO CONSILIARI (art. 125 del D.Lgs. 267/2000)

Si dà atto che gli estremi della presente deliberazione sono contenuti in un elenco che viene trasmesso oggi _____ ai Capigruppo consiliari.

f.to Il Segretario
Dr. Gino Prandini

CERTIFICATO DI ESECUTIVITA'

Certifico io sottoscritto Segretario comunale che la presente deliberazione diverrà esecutiva decorsi 10 giorni dalla pubblicazione ai sensi dell'art. 134, comma 3 del D.Lgs. 267/2000.

Lì _____

f.to Il Segretario
Dr. Gino Prandini

E' copia conforme all'originale da servire per uso amministrativo.

Lì _____

Il Segretario
Dr. Gino Prandini