FONDAZIONE
PER LO SPORT
DEL COMUNE DI
REGGIO EMILIA

Reggio Emilia, lì 31/07/2019

DETERMINAZIONE DEL DIRETTORE n. 2019/048

Estensore: Dott.ssa Giovanna D'Angelo

OGGETTO: Approvazione del modulo di implementazione delle misure minime di sicurezza ICT per le pubbliche amministrazioni in attuazione della circolare AGID n° 2/2017.

OGGETTO: Approvazione del modulo di implementazione delle misure minime di sicurezza ICT per le pubbliche amministrazioni in attuazione della circolare AgID n° 2/2017.

IL DIRETTORE

Premesso:

1. che con deliberazione di C.C. del Comune di Reggio Emilia N. 13602/181 del 13/07/2007, legalmente esecutiva, è stata approvata la Costituzione della "Fondazione per lo Sport" del Comune di Reggio Emilia e la partecipazione del Comune medesimo in qualità di Fondatore originario;

2. che con deliberazione di G.C. del Comune di Reggio Emilia n. 21739/278 del 23.10.2007 è stato approvato il relativo Statuto, successivamente modificato con deliberazione di G.C. N. 723/15 del 18/01/2012 e deliberazione notarile del Consiglio di Gestione della Fondazione n. 109.168 del 24/02/2012;

3. che con deliberazione di G.C. n. 22594/291 del 7.11.2007 è stato approvato il Protocollo d'intesa che regolamenta i rapporti tra il Comune di Reggio Emilia e la Fondazione per lo Sport, implicante la concessione gratuita alla Fondazione di vari immobili, tra cui alcuni impianti sportivi di proprietà comunale come modificato ed integrato con deliberazione di G.C. n. 20862/218 del 06/11/2012 e successivamente, con deliberazione di G.C. n. 80 I.D. del 30/04/2015;

4. che lo Statuto stabilisce all'art. 29 comma 3 che *"ai fini della individuazione delle funzioni e delle responsabilità del Direttore troveranno applicazione le disposizioni in materia di attribuzione di funzioni Dirigenziali previste dalla disciplina normativa degli Enti Locali, da intendersi qui convenzionalmente richiamata"*;

5. che nella seduta del 16 giugno 2008 il Consiglio di Gestione della Fondazione deliberava l'assegnazione delle funzioni di Direttore pro-tempore della Fondazione al dott. Domenico Savino, con decorrenza 1 gennaio 2008 e ciò fino al 31 dicembre 2009 e che nella seduta del 22 dicembre 2009 detto incarico veniva prorogato fino al 30 giugno 2010;

6. che con delibera n. 2 nella seduta del 25 marzo 2010 il Consiglio di Gestione della Fondazione deliberava di nominare ex art. 26, co. 1 dello statuto della Fondazione il dott. Domenico Savino alla carica di Direttore della Fondazione mediante assunzione con contratto a tempo indeterminato con decorrenza 1 luglio 2010;

Premesso:

- che a seguito del diffondersi in ambito pubblico di tecnologie informatiche di presidio ai processi, ai dati e alla gestione organizzativa degli Enti, anche le pubbliche amministrazioni sono divenute potenziali bersagli di attacchi informatici ai sistemi operativi e alle basi dati in questi contenute;

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

- che 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";

Visto:

- 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;

- 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 e che al fine di agevolare tale processo, ha individuato nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento;

- la Circolare di AgID del 18 aprile 2017, n. 2/2017 denominata "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni" che ha introdotto l'insieme dei controlli che costituiscono le Misure Minime AgID, denominati AgID Basic Security Controls (ABSC);

Considerato:

- che la pre-citata circolare prevede che 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 ed inviarlo al CERT-PA solo in caso di incidenti;

- che il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection

Regulation - Regolamento UE 2016/679) - pienamente applicato dal 25 maggio 2018 - intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea aumentando il livello di responsabilizzazione ed introducendo il concetto di misure idonee alle organizzazioni che sono chiamate ad attuare quanto necessario per la sicurezza informatica dei dati;

- che al fine di non costringere le Amministrazioni, soprattutto quelle più piccole, a disperdere risorse introducendo misure sproporzionate per la propria organizzazione, i controlli ABSC sono declinati come azioni puntuali di natura tecnica od organizzativa utili per valutare ed innalzare il proprio livello di sicurezza informatica;

- che i controlli ABSC sono suddivisi in tre gruppi verticali, riferiti a livelli complessivi di sicurezza crescente;

- che i controlli del primo gruppo (**livello "Minimo" M**) 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" S**) 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" A**) 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;

- che ogni Amministrazione deve 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 di protezione dei sistemi e delle infrastrutture tecnologiche;

Precisato:

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

  a) 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.

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

c) 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.

d) 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.

e) 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.

f) L'ottava ed ultima classe (ABSC13) 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.

Atteso:

- che gli Amministratori di sistema IT della Fondazione per lo Sport del Comune di Reggio Emilia sono stati nominati con disciplinari d'incarico professionale di cui ai prot. N. 177/E del 14/02/2018 e prot. N. 178/E del 14/02/2018;

- che gli Amministratori di sistema IT della Fondazione per lo Sport del Comune di Reggio Emilia ai sensi del Regolamento UE 679/2016 sono stati autorizzati a trattare i dati personali giacenti sui sistemi informatici della Fondazione con disciplinare di incarico di autorizzazione al trattamento dei dati di cui ai protocolli 2019/00214/E del 13/02/2019 e 2019/00226/E del 14/02/2019;

Preso atto:

- che gli amministratori di sistema della Fondazione per lo Sport del Comune di Reggio Emilia hanno predisposto e rassegnato al Direttore della Fondazione il Modulo di implementazione delle misure minime di sicurezza, allegato alla presente

determinazione dirigenziale (Allegato A), da sottoscrivere a cura del Direttore della Fondazione e del Legale Rappresentante;

Vista l'allegata dichiarazione di corretta istruttoria dell'atto, a firma dell'estensore dello stesso, Dott.ssa Giovanna D'Angelo, acquisita agli atti con prot. n. 2019/1097/E del 31/07/2019;

Tutto ciò premesso,

DETERMINA

1. di procedere alla sottoscrizione digitale del Modulo di implementazione delle Misure Minime di Sicurezza predisposta dagli Amministratori di Sistema della Fondazione per lo sport del Comune di Reggio Emilia (Allegato A);

2. di trasmettere il Modulo di implementazione delle Misure Minime di Sicurezza al Responsabile legale dell'Ente per la sua sottoscrizione;

3. di procedere successivamente alla protocollazione con marcatura temporale del Modulo di implementazione delle Misure Minime di Sicurezza della Fondazione per lo sport del Comune di Reggio Emilia al fine di dare attuazione agli adempimenti di cui all'art. 4 della Circolare AgID 18/04/2017, n.2/2017.

IL DIRETTORE
Dott. Domenico Savino
(documento firmato digitalmente)