Proponente: 33.A **Proposta: 2017/2418**	
del 29/12/2017	

COMUNE DI
REGGIO NELL'EMILIA

R.U.A.D. 1889
del 29/12/2017

GESTIONE E SVILUPPO DELLE TECNOLOGIE E DEI SISTEMI INFORMATIVI

Dirigente: BENEDETTI Dr.ssa Lorenza

PROVVEDIMENTO DIRIGENZIALE

OGGETTO: ATTUAZIONE DELLA CIRCOLARE AGID 18 APRILE 2017, N. 2/2017, RELATIVA ALLE MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI.

IL DIRIGENTE DEL SERVIZIO GESTIONE E SVILUPPO DELLE TECNOLOGIE E DEI SISTEMI INFORMATIVI

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";

Visto 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;

- la direttiva del 1° agosto 2015 del Presidente del Consiglio dei Ministri 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;

- la Circolare 18 aprile 2017, n. 2/2017 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) ha introdotto l'insieme dei controlli che costituiscono le Misure Minime AgID, denominati AgID Basic Security Controls (ABSC);

- 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, 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;

- il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679) - pienamente applicato entro il 25 maggio 2018 - 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 al fine di non costringere le Amministrazioni, soprattutto quelle più piccole, ad introdurre misure eccessive 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.

- 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.

Visto che:

- ad oggi non è ancora stato nominato dal Comune di Reggio Emilia il Responsabile per la transizione alla modalità operativa digitale di cui all'art 17 del D.Lgs 82/2005 come modificato dal D.Lgs 179/2016

- il Sindaco ha attribuito, con proprio provvedimento P.G. n. 38224 del 31/05/2016, incarico dirigenziale ad interim, sino alla scadenza del proprio mandato, del Sevizio Gestione e Sviluppo delle tecnologie e dei sistemi informativi alla Dott.ssa Lorenza Benedetti;

Preso atto:

- del modulo di implementazione delle misure minime di sicurezza predisposto dal Sevizio Gestione e Sviluppo delle tecnologie e dei sistemi informativi, allegato alla presente determina (Allegato A), da sottoscrivere a cura del Dirigente del Servizio Gestione e Sviluppo delle Tecnologie e dei sistemi informativi e del Legale Rappresentante;

Visto che :

sul presente provvedimento si esprime, con la sottoscrizione dello stesso, parere favorevole in ordine alla regolarità e correttezza dell'azione amministrativa come prescritto dall'art. 147 bis del D. Lgs. 267/2000;

Visti altresì:

- lo Statuto Comunale ed in particolare l'art.59;
- il D.Lgs. 267/2000;
- **i**l vigente Regolamento Generale degli Uffici e dei Servizi;

DETERMINA

1. di procedere alla sottoscrizione del Modulo di implementazione delle Misure Minime di Sicurezza predisposta dal Sevizio Gestione e Sviluppo delle tecnologie e dei sistemi informativi, (Allegato A);
2. di trasmettere il Modulo di implementazione delle Misure Minime di Sicurezza al Responsabile legale dell'Ente per la sottoscrizione al fine di dare attuazione agli adempimenti di cui all'art. 4 della Circolare AgID 18/04/2017, n. 2/2017;
3. di procedere alla conservazione del Modulo sottoscritto al fine di dare attuazione agli adempimenti di cui all'art. 4 della Circolare AgID 18/04/2017, n. 2/2017.

Si attesta inoltre che non sussistono situazioni di conflitto di interesse in capo al dirigente firmatario

IL DIRIGENTE DEL SERVIZIO

(D.ssa Lorenza Benedetti)

BENEDETTI LOR
2017.12.29 12:34:15
CN=BENEDETTI LORENZA
C=IT
O=COMUNE DI REGGIO N
2.5.4.5=IT:BNDLNZ68H65H
RSA/1024 bits

COMUNE DI
REGGIO NELL'EMILIA