CITTÀ DI CROTONE

Gabinetto del Sindaco

DECRETO N. 5 del 17/02/2023

Oggetto: **Nomina Amministratore di Sistema del Comune di Crotone.**

IL SINDACO

Visto il D.lgs. 30 giugno 2003, n. 196, "*Codice in materia di protezione dei dati personali*" e s.m.i.;
Visto il Regolamento (UE) 2016/679 recante disposizioni in materia di protezione dei dati personali;
Viste le disposizioni del Garante per la sicurezza dei dati personali ed in particolare il provvedimento del 27.11.2008, pubblicato nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, modificato con successivo provvedimento dello stesso Garante del 25 giugno 2009, pubblicato nella Gazzetta Ufficiale n. 149 del 30 giugno 2009;
Considerato che:

i provvedimenti citati disciplinano la figura dell' "*Amministratore di sistema*" (AdS), figura professionale deputata in ambito informatico alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali, e compresi i *client*, intesi come "postazioni di lavoro informatizzate", per cui devono essere registrati gli accessi;

Per *access log* si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software;

Gli *event records* generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "*username*" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato, ecc.).

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare o del Responsabile del Trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa

agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini) o tramite procedure formalizzate a istanza del lavoratore;

Dato atto che l'Amministratore di Sistema è tenuto a:

- svolgere il servizio con impegno, diligenza e professionalità, rispettando il codice di comportamento del Comune di Crotone;
- predisporre un *report* indicante i dettagli delle attività svolte;
- rispettare le norme in materia di tutela della salute e della sicurezza nei luoghi di lavoro ex D.lgs. n. 81/2008;
- osservare tutte le disposizioni conseguenti a leggi, regolamenti e decreti in vigore o emanati durante il periodo di durata del contratto, comprese ordinanze e regolamenti comunali;

Dato atto che l'incarico di Amministratore di Sistema ha per oggetto le seguenti attività:

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso all'interno del Comune;
- verificare il corretto funzionamento delle operazioni di *backup* e *recovery* dei dati e delle applicazioni;
- verificare l'idoneità dei sistemi di registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di "amministratore di sistema"); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- coordinamento delle attività finalizzate a identificare eventuali deficit tecnici e organizzativi dell'apparato comunale, indicazione di eventuali soluzioni correttive da intraprendere;
- Svolgimento delle funzioni di Amministratore di Sistema dell'Ente;
- Verifica delle misure minime di sicurezza, in conformità alla normativa in materia di privacy;
- Affiancamento dell'Ente nella definizione di politiche informatiche;
- Interfaccia tecnica tra l'Ente e i fornitori di hardware e software per l'individuazione delle migliori soluzioni tecniche, secondo il principio di efficacia ed economicità della spesa;
- Gestione del sistema di autenticazione informatica del personale dell'Ente;
- Gestione e assegnazione di adeguate *policy* di sicurezza di dominio, al fine di garantire criteri elevati di sicurezza sulla rete locale;
- Attribuzione di credenziali di autenticazione strutturate per mantenere caratteristiche di robustezza, inviolabilità nel rispetto della segretezza della componente riservata della credenziale di autenticazione ai sensi della normativa vigente con correlata attività di informazione dei dipendenti comunali in ordine alle metodiche di gestione delle credenziali, al fine di garantire la salvaguardia dei requisiti di disponibilità, integrità e riservatezza dei dati;
- Gestione del sistema di autorizzazione informatica e predisposizione di adeguati profili secondo l'organizzazione degli uffici e dei servizi;
- Analisi delle procedure per l'adozione di sistemi di protezione contro il rischio di intrusione e dell'azione di programmi ex art 615 quinquies c.p.;
- Verifica di idonee politiche finalizzate al trattamento centralizzato dei dati su apparecchiature informatiche preventivamente individuate e appositamente predisposte;
- Verifica dell'idoneità delle politiche di backup, finalizzate all'esecuzione codificata di copie di sicurezza dei dati trattati, su supporti di archiviazione indipendenti e fisicamente separati rispetto

ai sistemi informatici che formano oggetto di backup;
- Verifica di idonee procedure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;
- Supporto per l'individuazione e l'adozione di un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte dell'Amministratore di Sistema;
- Continuità operativa dell'Ente e *Disaster Recovery*, in caso di evento dannoso, personalizzata in base alle necessità e alle disponibilità economiche dell'Amministrazione Comunale;
- Dimensionamento postazioni informatiche presenti o di futura installazione;
- Verifica di idonea installazione ed aggiornamento di antivirus e firewall necessari per l'implementazione e l'adeguamento del sistema informatico comunale;
- Supporto nell'individuazione di eventuali strumenti tecnici necessari per l'informatizzazione di procedure e processi dell'Ente;
- Analisi funzionale dei sistemi informatici operativi sulla rete interna dell'Ente, atta ad identificare e sanare eventuali criticità tecniche ed organizzative;
- Supporto informatico agli incaricati del trattamento dei dati circa il corretto uso della propria postazione di lavoro, di internet, della posta elettronica e degli altri strumenti elettronici utilizzati per fini lavorativi nel rispetto di quanto previsto dalla normativa vigente;
- Supporto nell'installazione e configurazione dei software specifici per la pubblica amministrazione (es. Desktop Telematico, Entratel, Saia-Client, Isi-Istatel, BDNA, etc.);
- Supporto nell'installazione, configurazione ed utilizzo dei software e dei dispositivi di firma digitale;
- Supporto all'installazione o ripristino di sistemi operativi, software antivirus, pacchetti applicativi purché gli stessi siano corredati dei relativi supporti di installazione originali e dotati di regolare licenza di utilizzo;
- Configurazione apparati di stampa e scansione sulla rete locale e sulle singole postazioni di lavoro;
- Assistenza diretta, telefonica e teleassistenza;

Ritenuto opportuno individuare la figura di Amministratore di sistema nei termini che precedono l'Ing. Salvatore Greco, istruttore direttivo informatico di categoria D, assegnato all'Ufficio 4.1.4 del Settore 4;

Visto il Regolamento (UE) 2016/679 recante disposizioni in materia di protezione dei dati personali;
Viste le disposizioni del Garante per la sicurezza dei dati personali ed in particolare il provvedimento del 27.11.2008, pubblicato nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, modificato con successivo provvedimento dello stesso Garante del 25 giugno 2009, pubblicato nella Gazzetta Ufficiale n. 149 del 30 giugno 2009;
Visto il Regolamento Europeo UE 2016/679;
Visto l'art. 50 del TUEL;
Visto lo Statuto Comunale;
Per quanto sopra premesso e motivato,

DECRETA

1. la premessa è richiamata nel dispositivo per farne parte integrante;
2. **di nominare** Amministratore di sistema nei termini descritti in premessa l'Ing. Salvatore Greco, istruttore

direttivo informatico di categoria D, assegnato all'Ufficio 4.1.4 del Settore 4;
3. **di dare atto** che l'incarico di Amministratore di Sistema ha ad oggetto le attività analiticamente indicate in premessa;
4. **di specificare** che il presente atto non comporta spese rientrando nelle mansioni esigibili rientranti, sulle base delle disposizioni contrattuali, tra le mansioni proprie della categoria D;
5. **di dare atto** che il provvedimento produce effetti dalla data di accettazione;
6**. di disporre** che il presente provvedimento sia:
a) notificato all'Ing. Salvatore Greco che provvederà a sottoscriverlo per accettazione;
b) trasmesso alla Dott.ssa Melania Muraca, quale Responsabile della protezione dei dati (RDP/DPO) del Comune di Crotone;
c) trasmesso per opportuna conoscenza al Segretario Generale e a tutti i Dirigenti;
d) trasmesso, in particolare, al Dirigente del Settore 1 "Affari generali e servizi trasversali all'Ente", affinché proceda all'informativa destinata ai lavoratori dell'Ente, prevista dalla normativa vigente in materia di protezione dei dati e dallo Statuto dei lavoratori;
e) pubblicato all'albo pretorio informatico e sul sito istituzionale del Comune www.comune.crotone.it nell'apposita sezione "Amministrazione trasparente", sottosezione di primo livello "Altri contenuti", sottosezione di secondo livello "Dati ulteriori".

Il Sindaco

f.to Ing. Vincenzo Voce

firme autografe sostituite a mezzo stampa ai sensi dell'art. 3, comma 2, del D.Lgs .n. 39/1993