Movimento 5 Stelle Trepuzzi

Trepuzzi, 1 agosto 2019

Al Sindaco del Comune di Trepuzzi
Dott. Giuseppe Maria Taurino

Al Presidente del Consiglio Comunale di Trepuzzi
Dott. Alessandro Capodieci

Oggetto: **Interrogazione, ai sensi dell'art. 56 comma 4 del Regolamento del Consiglio Comunale, in merito a "Sorveglianza del Palazzo Comunale e Continuità dei Sistemi Informativi".**

Il sottoscritto **Massimo SCARPA**, in qualità di consigliere comunale del Comune di Trepuzzi, propone la seguente interrogazione secondo quanto specificato:

PREMESSO che:

- alle Pubbliche Amministrazioni spetta il compito di garantire in maniera continuativa l'erogazione dei servizi ai cittadini e alle imprese. Per poter adempiere a tale compito, le PA devono, in particolare, garantire la sicurezza dei luoghi ove insistono tutte le infrastrutture tecnologiche/logistiche necessarie all'espletamento dei vari servizi. Ovvero, le PA dovrebbero mettere in atto anche opportuni servizi di sorveglianza degli immobili comunali;

- a fronte di emergenze di qualunque natura, che potrebbero compromettere la regolare offerta di servizi da parte della PA, l'ente deve esprimere una capacità organizzativa atta a salvaguardare l'operatività dell'ente stesso;

- nell'ambito della sicurezza informatica, per Disaster Recovery si definisce il processo organizzativo e logistico che, a seguito di un'emergenza, consenta il ripristino delle infrastrutture necessarie all'erogazione dei servizi di business per enti e cittadini. In particolare, il piano di DR deve prevedere l'utilizzo temporaneo di un Centro Elaborazione Dati alternativo oppure l'utilizzo di sistema di assistenza da utilizzare in attesa del ripristino. Invece, per Continuità Operativa si intende l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale;

- la ditta PARSEC 3.26 SRL gestisce il servizio di assistenza e manutenzione del Sistema Informatico/vo Comunale 2019.

CONSIDERATO che:

- la notte del 21 marzo 2019 scorso, nella sede principale del Comune di Trepuzzi, ovvero nel Palazzo comunale di

via Garibaldi, si sono introdotti degli individui che hanno messo a soqquadro diversi uffici e hanno sottratto sette computer con i relativi monitor;

- durante la riunione della I^ Commissione Consiliare tenutasi il **15 maggio 2019**, avente tra i punti all'ordine del giorno la discussione del BILANCIO DI PREVISIONE FINANZIARIO 2019-20121, lo scrivente ha domandato se la sicurezza, ovvero il servizio di sorveglianza del Palazzo Comunale fosse affidato a qualche Istituto di vigilanza;

- le indicazioni fornite dal Sindaco, alla domanda di cui al precedente punto, sono state le seguenti:
"c'è il contratto con la Vigile. La videocamera è collegata con la Polizia Municipale. Viene monitorata e registrata.... Noi abbiamo un contratto su alcuni immobili comunali. Non ricordo se rientra pure questo. .. le scuole sono collegate... " ;

- dal Bilancio di Previsione finanziario 2019-2021, per il capitolo di spesa MANUTENZIONE ORDINARIA E SERVIZIO DI VIGILANZA (2320003) è stata prevista una spesa di € 5.000 per il 2019, 2020 e 2021;

- nel 2018 risulterebbero imputate, ovvero liquidate, per servizi di vigilanza le seguenti spese

Cap di Spesa	Servizio	N° Determina	Importo Liquidato	Beneficiario
1470001	PROGETTO **BIBLIOTECHE** SCOLASTICHE INNOVATIVE-PIANO NAZIONALE SCUOLA DIGITALE-IMPIANTO **DI SICUREZZA IST.COMPR.STATALE POLO 1**	33	€ 1.449,36	ditta la Vigile Security Service
2320003	SERVIZIO ANNUALE DI COLLEGAMENTO IMPIANTO ALLARME TOP PRESSO **PISCINA COMUNALE**	753	€ 1.242,94	ditta la Vigile Security Service
2320003	SERVIZIO DI COLLEGAMENTO SISTEMA D'ALLARME TOP PRESSO CENTRO **SOCIALE ZONA SANTI**	754	€ 500,00	ditta la Vigile Security Service

- l'infrastruttura ICT del Comune di Trepuzzi è distribuita su n.2 sedi (Palazzo Comunale e sede del Comando di Polizia Municipale);

- nell'architettura informatica è fondamentale il ruolo delle componenti di STORAGE deputate alle attività di backup. Esse, infatti, in caso di incidenti (*incendi, alluvioni,...*) consentono il ripristino dei dati delle applicazioni utilizzate per fornire servizi ai cittadini ed ai vari enti;

- nell'ambito della sicurezza informatica, le attività svolte dalle PA rispondono a norme che hanno valore legale. Le norme più rilevanti sono contenute nel **Codice dell'Amministrazione Digitale** (CAD – D.Lgs. 7 marzo 2005 s.m.i.) In particolare l'Art. 17 (*Responsabile per la transizione digitale e difensore civico digitale*) prevede che le pubbliche amministrazioni individuino mediante propri atti organizzativi, un unico ufficio dirigenziale generale responsabile del coordinamento funzionale;

- l'Art. 2. *Finalità e ambito di applicazione* del **Codice dell'amministrazione digitale (CAD)** prevede al comma 1 - *"Lo Stato, le Regioni e le autonomie locali assicurano la **disponibilità**, la gestione, l'accesso, la trasmissione, **la conservazione e la fruibilità dell'informazione in modalità digitale** e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti le tecnologie dell'informazione e della comunicazione"-;*

- la riforma Madia (D.Lgs. n 179 2016 all'art 64 1 comma lett h) ha abrogato l'Art. 50 bis (*Continuità operativa*)

del CAD che stabiliva gli adempimenti a carico delle PA rispetto alla predisposizione di piani di continuità operativa e di disaster recovery. In particolare, l'art 50 bis del CAD al comma 3 indicava:
3. A tali fini, le pubbliche amministrazioni definiscono:
*a) **il piano di continuità operativa**, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità.....*
*b) **il piano di disaster recovery**, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.....*

Per questo DigitPA aveva indicato le linee guida atte a fornire gli strumenti per realizzare gli obblighi di cui sopra attraverso idonee soluzione tecniche;

- l'Art. 51. *Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni* del **Codice dell'amministrazione digitale** (CAD) prevede al comma 1 quanto segue
*-"1.Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le soluzioni tecniche idonee a garantire **la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture**"-.*
Mentre al comma 2 prevede:
*-"2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da **ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito** o non conforme alle finalità della raccolta"-.*

VISTO che:

- il Palazzo comunale di Trepuzzi risulterebbe sprovvisto del servizio di vigilanza;

- dal documento dell'***offerta servizio di assistenza e manutenzione Sistema Informatico/vo Comunale 2019***, della Parsec 3.26 S.r.l. società di informatica, in particolare dallo schema dell'infrastruttura in esso rappresentato, risulta che la componente di Backup sia installata presso la sala CED che insiste nel palazzo Comunale. Pertanto, non risulterebbero essere previste misure tecnologiche idonee al "*Recupero dal Disastro*" (Disaster recovery); ovvero, misure capaci, a fronte di gravi incidenti sull'intera infrastruttura informatica, di ripristinare applicazioni, sistemi/infrastrutture e dati necessari alla corretta erogazione dei servizi.

RITENUTO che:

- a fronte di incidenti/inconvenienti di qualsiasi natura, il sistema informatico/vo e in particolare le componenti di backup potrebbero essere danneggiate anche irrimediabilmente. Ciò potrebbe pregiudicare il ripristino delle normali operazioni di servizio e quindi delle attività degli uffici. Pertanto sarebbe auspicabile l'installazione di un servizio di backup remoto (p.e. in cloud) parallelamente al backup locale;

- anche in mancanza di una chiara normativa è evidente che un ente pubblico è tenuto a predisporre un preciso piano di disaster recovery e di continuità operativa. La mancanza di tale piano implicherebbe, infatti, una precisa responsabilità da parte dell'ente in quanto la continuità dei servizi delle pubbliche amministrazioni rappresenta comunque un obbligo istituzionale.

- a fronte di danni prolungati nel tempo dell'infrastruttura informatica, la mancata applicazione di un piano di continuità operativa e quindi l'impossibilità di fornire servizi per un periodo significativo di tempo potrebbe esporre il Comune di Trepuzzi a possibili denunce dei cittadini e richieste di risarcimenti danni.

CHIEDE:

- quale tipo di sorveglianza, oltre l'impianto di videosorveglianza collegato con la sede della Polizia Municipale, esiste a garanzia della sicurezza e protezione del palazzo comunale;

- se è previsto l'affidamento del servizio di vigilanza del palazzo comunale;

- dove vengono custoditi i backup (che sono registrati su QNAP TS-269L). Ovvero, se i backup sono custoditi solo nei locali dei server;

- se parallelamente al backup locale dei server principali è previsto un servizio di backup remoto (p.e. in Cloud). Ovvero, se, qualora il servizio di backup remoto non fosse stato già attivato, è intenzione dell'amministrazione provvedere in tal senso;

- se oltre le azioni previste dall'attuale **servizio di assistenza e manutenzione Sistema Informatico/vo Comunale** la giunta prevede di impegnarsi ad avviare la predisposizione di un preciso piano di disaster recovery e di continuità operativa.

Ringrazio e porgo cordiali saluti.

Firma

Massimo Seoyc