PROTOCOLLO D'INTESA TRA COMUNE DI BOLOGNA, CITTA' METROPOLITANA DI BOLOGNA E I COMUNI DELL'AREA METROPOLITANA DI BOLOGNA IN MATERIA DI SICUREZZA INFORMATICA

Premesso che:

le minacce cibernetiche, hanno assunto una rilevanza sempre maggiore e nell'ultimo anno, il 2021, gli attacchi nel mondo sono aumentati del 10% rispetto all'anno precedente. Le capacità di penetrazione degli attacchi cyber sono sempre più sofisticate e va segnalato anche l'aumento del numero di attacchi informatici ad alto impatto, con effetti a livello politico e geopolitico, oltre che economico.
Gli attacchi verso l'Europa rappresentano circa il 21%, un quinto del totale mondiale. La diffusione degli attacchi cibernetici riguarda obiettivi multipli e in Italia tra i settori interessati, anche nel 2021, la Pubblica Amministrazione si conferma essere quello più colpito.
Nel territorio metropolitano di Bologna le minacce hanno assunto un rilievo particolarmente sentito. Nel corso del 2021, due Unioni di comuni, hanno subito attacchi informatici molto gravi, che hanno portato alla cosiddetta "esfiltrazione" di rilevanti quantità di dati ed al blocco per più giornate dei sistemi informativi e quindi di tutte le attività di ufficio, dei comuni interessati. La sicurezza informatica è quindi una emergenza a tutti livelli istituzionali e rappresenta una priorità all'interno delle strategie di sviluppo dell'Unione europea.
A tal fine la Commissione europea, nell'ambito di una direttiva sulle misure per un elevato livello comune di cybersicurezza (direttiva NIS e NIS 2), ha proposto a tutti i paesi membri dell'Unione di riformare le norme sulla sicurezza delle reti e dei sistemi informatici al fine di aumentare il livello di tutela dei settori pubblici e privati essenziali, strutture ospedaliere, reti energetiche, ferrovie, centri dati, amministrazioni pubbliche, laboratori di ricerca e produzioni di dispositivi medici e medicinali, altre infrastrutture essenziali, che devono rimanere protetti a fronte di minacce repentine e sempre più complesse.
La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.
Successivamente, il decreto-legge n. 105 del 2019 è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un **perimetro di sicurezza nazionale cibernetica** e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione.
La sicurezza cibernetica costituisce, uno degli interventi principali previsti dalla Missione1 (Digitalizzazione, innovazione e sicurezza nella P.A.) del **Piano nazionale di ripresa e resilienza (PNRR) ,** all'interno della quale si inseriscono anche gli specifici obiettivi del Piano Italia Digitale 2026.

Visto che

1 La Missione 1 del PNRR, "Digitalizzazione, innovazione e sicurezza nella P.A.", mira a trasformare profondamente in chiave digitale la Pubblica Amministrazione italiana, con l'obiettivo di renderla "la migliore alleata dei cittadini e delle imprese". Una trasformazione digitale che segue l'approccio Cloud first, orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni verso un ambiente *cloud*, attraverso la

creazione del **Polo strategico nazionale ed il processo di certificazione dei provider dei servizi cloud per la PA**, superando così le attuali carenze di requisiti minimi di sicurezza e affidabilità. Una trasformazione finalizzata alla piena attuazione della disciplina in materia di "Perimetro di sicurezza nazionale Cibernetica" che insieme all'adozione del Decreto-legge n. 82/2021 e l'istituzione dell'Agenzia per la cybersicurezza nazionale confermano in maniera definitiva e coerente con le indicazioni della Commissione europea, la rilevanza nazionale che ricopre la cybersecurity. Tuttavia, se il percorso di migrazione in ambito cloud e di adozione delle misure di cybersecurity delle amministrazioni centrali appare più definito, nel caso gli enti locali minori, emergono importanti criticità, legate all'insufficiente "*massa critica"* per una gestione individuale di servizi cybersecurity. In questi casi il PNRR prevede come soluzione obbligatoria, l'aggregazione di enti locali in raggruppamenti ad hoc per l'esecuzione di attività di trasformazione/migrazione dei servizi nel Polo strategico nazionale o presso i provider certificati. Per accompagnare la migrazione è previsto un programma di supporto e incentivo per trasferire basi dati e applicazioni, in particolare rivolto alle amministrazioni locali.

2 Una seconda criticità legata alla migrazione dei servizi digitali in cloud e all'adozione delle misure di cybersicurezza, riguarda la necessità del rafforzamento e rinnovo delle competenze digitali del personale della Pubblica Amministrazione. Risulta quindi indispensabile avviare percorsi di formazione del personale, in ambito cyber security, indirizzati su due azioni principali:

- un intervento formativo diffuso per tutti i dipendenti pubblici (Comuni, Unioni del territorio, realtà sanitarie e Regione stessa), in grado di integrare e rafforzare gli strumenti già esistenti o in fase di realizzazione a livello regionale (si veda la piattaforma Self PA) e nazionale (iniziative del Formez, Forum PA, eccetera) mediante il coordinamento e l'arricchimento degli strumenti disponibili, possibilmente in collaborazione con l'Università e gli altri livelli di istruzione rilevanti su questo argomento.

- una azione territoriale di sistema, per la creazione di figure tecniche specialiste competenti sulla cybersecurity per la pubblica amministrazione, attualmente non disponibili sul mercato del lavoro, indispensabili per potenziare all'interno degli enti le strutture dedicate alla sicurezza informatica. Queste figure andranno ad affiancare i tecnici che già sono in campo all'interno delle strutture dedicate alla gestione dei servizi informatici degli enti, allargando le competenze in dotazione agli enti locali per la gestione della sicurezza informatica.

Le parti sottoscrittici si impegnano reciprocamente a:

1 Condividere, in coerenza con le suddette premesse, la necessità e l'urgenza di un innalzamento delle difese di sicurezza informatica dedicate alla protezione delle loro infrastrutture digitali e dei servizi pubblici come indicato nella Missione 1 del PNRR.

2 Creare un percorso condiviso, eventualmente attraverso la formalizzazione di una aggregazione di enti locali (tale da costituire la "*massa critica",* come indicato dal PNRR), per avviare la migrazione dei loro servizi digitali all'interno del cloud della pubblica amministrazione.

3 Agire di concerto, in forme da individuare, per il reclutamento di nuovo personale tecnico esperto in cybersecurity, necessario alla riorganizzazione dei servizi di sicurezza informatica.

4 Promuovere percorsi innovativi per il reclutamento e la formazione di nuovo personale per i servizi di sicurezza informatica, attraverso lo strumento del corso-concorso per la selezione e avviando in collaborazione con gli Istituti tecnici superiori un percorso per la formazione di tecnico specialista in sicurezza informatica per la pubblica amministrazione.

5 Costituire un comitato di coordinamento del progetto con referenti individuati dagli enti sottoscrittori del presente protocollo di intesa e che la sua composizione può essere modificata con una comunicazione tra le Parti senza modificare il presente protocollo di intesa.

6 Rendersi disponibili ad avviare percorsi di collaborazione e a condividere esperienze con altre aggregazioni di enti locali, che si possono costituire nella Regione Emilia-Romagna e in altre regioni italiane che intendono avviare percorsi simili d'innovazione digitale e di cybersecurity.

7 Prestare particolare attenzione alla necessità di competenze tecniche specialiste nel campo della cybersecurity espresse anche dal mondo dei servizi e delle imprese del territorio metropolitano bolognese. A tal fine si rendono disponibili a valutare collaborazioni innovative di carattere pubblico-privato per la diffusione e l'innalzamento delle competenze digitali.

Bologna, …..

Per il Comune di Bologna

_____

Per la Città metropolitana di Bologna

_____

Per il Comune di _____