



CITTA' DI TORINO

**DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY**

ATTO N. DEL 74

Torino, 21/02/2023

DELIBERAZIONE DELLA GIUNTA COMUNALE

Convocata la Giunta, presieduta dalla Vicesindaca Michela FAVARO, sono presenti gli Assessori:

Domenico CARRETTA	Carlotta SALERNO
Paolo CHIAVARINO	Jacopo ROSATELLI
Chiara FOGLIETTA	Rosanna PURCHIA
Paolo MAZZOLENI	Giovanna PENTENERO
Gabriella NARDELLI	Francesco TRESSO

Assente, per giustificati motivi, il Sindaco Stefano LO RUSSO.

Con l'assistenza della Segretaria Generale Rosa IOVINELLA.

OGGETTO: PNR - AMBITO DELL'INVESTIMENTO 1.5 "CYBERSECURITY"- MISSIONE MIC1 - "ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAMENTO NELLA GESTIONE DEI PROCESSI LEGATI ALLA CYBERSECURITY DELLA CITTA' DI TORINO CUP C17H22002830006" E "CYBERSECURITY: INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO NELLA CITTA' DI TORINO CUP C17H22002840006" - PRESA D'ATTO AMMISSIONE AL FINANZIAMENTO PER COMPLESSIVI EURO 1.990.200,00 ED APPROVAZIONE ATTI D'OBBLIGO REGOLANTI I RAPPORTI TRA L'ACN E LA CITTA' DI TORINO. FINANZIAMENTO NEXT GENERATION EU.

Visto che in data 14/10/2022 la Città ha aderito all'Avviso pubblico approvato con det. prot. N. 010220 del 29/07/2022 dell'Agenzia per la Cybersicurezza Nazionale (ACN) - (All.1), per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei

Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, Missione 1 - Componente 1- Investimento 1.5. "Cybersecurity" M1C1I1.5, presentando i seguenti progetti:

- “Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino”, euro 995.100,00 CUP C17H22002830006 - (All. 2);
 - “Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino” euro 995.100,00 CUP C17H22002840006 - (All. 3);
- Visto che con det prot. N. 3429 del 20/01/2023 l’Agenzia per la Cybersicurezza Nazionale (ACN) ha approvato la graduatoria finale e le progettualità del Comune di Torino sono entrambe risultate ammesse e totalmente finanziabili.

Premesso che il sistema informativo della Città di Torino è composto dalle risorse tecnologiche, le risorse organizzative e il portafoglio di applicazioni. La missione del sistema informativo è quella di realizzare, con nuove tecnologie, un sistema efficiente, che semplifica le procedure e mette in comune le informazioni raccolte.

Il primo progetto, denominato “Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino” - CUP C17H22002830006, prevede interventi di potenziamento della propria infrastruttura, attraverso l’adozione ed il miglioramento di capacità cyber in essere, per identificare, anticipare e rispondere alle nuove forme di minaccia che caratterizzano l’evoluzione tecnologica dei sistemi informativi.

Nello specifico, i vari interventi rientrano nelle seguenti tipologie:

- analisi della postura di sicurezza e piano di potenziamento, che consiste nell’acquisizione di un servizio che prevede attività per individuare il livello di maturità delle capacità cyber dei servizi informativi, attraverso un’analisi approfondita della contestualizzazione del *framework* nazionale di cybersecurity al contesto dell’Amministrazione e la definizione dei relativi livelli di priorità e di maturità. L’obiettivo è quello di fornire uno strumento di autovalutazione del rischio cyber, perseguendo l’obiettivo di valutare il rischio cyber all’interno di un tipico scenario dell’Amministrazione, così come la valutazione ad alto livello dell’impatto economico dell’implementazione delle misure del *framework* nazionale. Infine, il servizio, sulla base dei risultati ottenuti, prevede la definizione di un piano di *remediation*, al fine di effettuare una pianificazione strategica delle azioni di contenimento ed un piano di potenziamento delle capacità cyber.
- miglioramento dei processi e dell’organizzazione di gestione della cybersecurity, che consiste nell’acquisizione di un servizio che prevede la definizione di policy, procedure organizzative ed operative di gestione degli incidenti informatici, analisi dei processi interni in particolar modo nell’ambito della gestione della continuità operativa e della gestione delle vulnerabilità, nonché nell’acquisizione di un supporto nella definizione, configurazione ed erogazione di servizi di monitoraggio continuo delle vulnerabilità di sicurezza per ottenere un miglioramento ed un potenziamento dei processi stessi.

Il secondo progetto, denominato "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino" - CUP C17H22002840006, prevede invece interventi di potenziamento della propria infrastruttura, attraverso l’adozione ed il miglioramento di capacità cyber in essere, per identificare, anticipare e rispondere alle nuove forme di minaccia che caratterizzano l’evoluzione tecnologica dei sistemi informativi.

Nello specifico, i vari interventi rientrano nelle seguenti tipologie:

- miglioramento della consapevolezza delle persone, che consiste nell’acquisizione di un servizio che prevede la predisposizione di sessioni di formazione su svariati aspetti della sicurezza delle informazioni, allo scopo di incrementare il livello di consapevolezza dei dipendenti, innalzando il

livello di sicurezza dell'organizzazione e l'efficacia in termini di protezione dei dati critici e dei dati personali. Il servizio sarà erogato da specialisti del settore anche attraverso l'adozione di una piattaforma tecnologica per l'erogazione dei contenuti in modalità *e-learning* e per gestire campagne di simulazione di *phishing*.

- progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber, e consiste nell'acquisizione di un servizio che prevede la revisione e gestione delle policy di sicurezza sui sistemi di protezione perimetrale ed applicativo dell'Amministrazione, l'acquisizione di nuovi servizi e piattaforme di sicurezza per il monitoraggio degli eventi di sicurezza, l'individuazione di nuove vulnerabilità, la protezione della navigazione internet e della posta elettronica, la protezione ed il monitoraggio continuo delle postazioni di lavoro, la gestione delle identità e degli accessi allo scopo di elevare la capacità di risposta dell'Amministrazione in caso di incidente.

Considerato che l'Avviso pubblico prevede la sottoscrizione dell'Atto d'obbligo secondo lo schema di cui all'All. C dell'avviso stesso.

Con gli atti d'obbligo la Città di Torino, in qualità di soggetto attuatore, dichiarando di aver preso visione della determina n. 3429 del 18/01/2023 (All. 4) adottata dall'Agenzia per la Cybersicurezza Nazionale di cui sopra, accetta espressamente e integralmente tutti i termini, obblighi e condizioni ivi previste.

In particolare, gli atti d'obbligo prevedono che al fine di assicurare il rispetto degli obiettivi intermedi e finali (milestones e target) il soggetto attuatore si impegni a:

- avviare gli interventi a partire dalla data di sottoscrizione e ricezione degli stessi atti;
- portare a termine e completare le attività entro la data indicata nei Piani di Progetto, ovvero nella diversa data eventualmente concordata con l'Agenzia per la Cybersicurezza Nazionale con puntuale aggiornamento dei medesimi Piani di Progetto (All. 5 e 6)
- trasmettere all'Agenzia per la Cybersicurezza Nazionale, nelle modalità previste dall'Avviso, entro e non oltre 30 giorni naturali e consecutivi dalla conclusione del progetto, al fine di consentire l'ammissibilità del contributo, la documentazione finale attestante le spese sostenute.

Dato atto che sono previste le seguenti modalità di erogazione dei contributi:

- Anticipo pari al 10% del contributo totale ammesso a finanziamento, a seguito della sottoscrizione degli Atti d'obbligo;
- Erogazione di tranches di rimborso (fino al 90% del contributo inclusa l'anticipazione) previa presentazione di domande di rimborso intermedie, che dimostrino l'avanzamento nell'attuazione della progettualità con riferimento alle spese ed all'avanzamento nel conseguimento del target in coerenza con la scadenza concordata con l'Unione europea (dicembre 2024), relativamente alla quota parte di competenza del progetto;
- Erogazione a saldo previa presentazione della domanda di rimborso saldo finale, a seguito del completamento dell'intervento e del comprovato conseguimento del target, relativamente alla quota parte di competenza del progetto, entro la relativa scadenza concordata con l'Unione europea (dicembre 2024).

Con il presente provvedimento, si rende pertanto necessario approvare i due Atti d'Obbligo, uno per ciascuna progettualità, che saranno sottoscritti dal Sindaco e che sono allegati al presente atto per farne parte integrante e sostanziale (All. 7-8), con i quali la Città si impegna a garantire il rispetto dei tempi, delle modalità e degli obblighi relativi all'attuazione delle proposte progettuali.

Dato atto che il presente provvedimento per la natura dell'oggetto non è pertinente alle disposizioni in materia di valutazione dell'impatto economico; la relativa dichiarazione alla valutazione dell'impatto economico sarà resa in sede di specifica approvazione degli atti previsti per ciascun

singolo intervento.

Tutto ciò premesso,

LA GIUNTA COMUNALE

Visto l'art. 48 del Testo Unico delle leggi sull'Ordinamento degli Enti Locali, approvato con D.Lgs. 18 agosto 2000 n. 267.

Dato atto che i pareri di cui all'art. 49 del suddetto Testo Unico sono:

- favorevole sulla regolarità tecnica;
- favorevole sulla regolarità contabile;

Con voti unanimi, espressi in forma palese;

DELIBERA

per le motivazioni espresse in narrativa, che integralmente si richiamano;

1. di prendere atto dell'ammissione al finanziamento nell'ambito del PNRR M1C1 - Digitalizzazione, Innovazione e Sicurezza nella PA” - Investimento 1.5 "Cybersecurity", dei due progetti denominati “Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino” - CUP C17H22002830006 - per euro 995.100,00 e “Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino” - CUP C17H22002840006 - per euro 995.100,00;
2. di approvare i due Atti d'Obbligo, uno per ciascuna progettualità, redatti secondo lo schema di cui all'allegato C dell'Avviso Pubblico (All. 1) di cui sopra, che saranno sottoscritti dal Sindaco e che sono allegati al presente atto per farne parte integrata (All. 7 - 8), con i quali la Città si impegna a garantire il rispetto dei tempi, delle modalità e degli obblighi relativi all'attuazione delle proposte progettuali;
3. di rinviare a successivi provvedimenti dirigenziali quanto necessario all'avvio degli interventi nel rispetto dei cronoprogramma e delle procedure previste;
4. di dare atto che il presente provvedimento per la natura dell'oggetto non è pertinente alle disposizioni in materia di valutazione dell'impatto economico;
5. di dichiarare, attesa l'urgenza, in conformità del distinto voto palese ed unanime, il presente provvedimento immediatamente eseguibile ai sensi dell'art. 134, 4° comma, del Testo Unico approvato con D.Lgs 18 agosto 2000 n. 267, in quanto al fine del rispetto dei termini previsti, occorre dare avvio tempestivamente alle procedure per la realizzazione dell'intervento.

Proponenti:

IL SINDACO
Stefano Lo Russo

LA ASSESSORA
Giovanna Pentenero

Si esprime parere favorevole sulla regolarità tecnica.

IL DIRIGENTE

Massimo Massimino

Si esprime parere favorevole sulla regolarità contabile.

LA DIRIGENTE FINANZIARIA
Patrizia Rossini

LA VICESINDACA
Firmato digitalmente
Michela Favaro

LA SEGRETARIA GENERALE
Firmato digitalmente
Rosa Iovinella

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire ¹, archiviati come file separati dal testo del provvedimento sopra riportato:

1. DEL-74-2023-All_1-Avviso_Pubblico.pdf 
2. DEL-74-2023-All_2-Allegato_A1_Domanda_di_ammissione_PAL_Progetto_1_signed.pdf 
3. DEL-74-2023-All_3-Allegato_A1_Domanda_di_ammissione_PAL_Progetto_2_signed.pdf 
4. DEL-74-2023-All_4-Det_3429_ammissione_finanziamento.pdf 
5. DEL-74-2023-All_5-Allegato_B_Piano_di_Progetto_PAL_Progetto_1_signed.pdf 
6. DEL-74-2023-All_6-Allegato_B_Piano_di_Progetto_PAL_Progetto_2_signed.pdf 
7. DEL-74-2023-All_7-
ATTO_D'OBBLIGO_ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAMENTO NEL
LA_GESTIONE_DEI_PROCESSI_LEGATI ALLA CYBERSECURITY.pdf 
8. DEL-74-2023-All_8-
ATTO_D'OBBLIGO_INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E S
VILUPPO_NUOVI_SISTEMI_PER_LA_MITIGAZIONE_DEL_RISCHIO_NELLA_CITTÀ_DI_TORI
NO.pdf 

¹ L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento