

## **CITTÀ METROPOLITANA DI GENOVA**

### **SCRITTURA PRIVATA**

#### **MODIFICA CONTRATTO DI APPALTO ID.2024\_169**

##### **Ai sensi dell'art.120 del D. Lgs.36/2023**

del Contratto di appalto ID.2024\_169 PNRR M1C1I1.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU avente ad oggetto affidamento in house ai sensi dell'art. 7 del D. Lgs. 36/2023 del servizio di consulenza e acquisto forniture per l'attuazione del progetto "CYBER CMGE"- CUP D41B20001480006 - CIG B451B6CDF8.

#### **TRA**

La Città Metropolitana di Genova (C.F. 80007350103), di seguito denominata anche "Amministrazione", rappresentata dalla dott.ssa Laura Papaleo, nata a [REDACTED] nella sua qualità di Dirigente del Servizio Strategie digitali, ICT e finanziamenti europei;

#### **E**

L'operatore economico Liguria Digitale S.p.A. (P.IVA 02994540108) avente sede in Genova, Via Melen 77, di seguito denominato anche "Affidatario" rappresentato Lorenzo Rizzo nato a [REDACTED] e Alessandro Lino nato a [REDACTED] loro qualità di Procuratori Speciali di Liguria Digitale;

#### **VISTI:**

- il D. Lgs. 31 marzo 2023, n. 36, Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici e in particolare, e in particolare l'articolo 120 "Modifica dei contratti in corso di esecuzione";
- l'atto dirigenziale n. 3011 del 22/11/2024 avente ad oggetto "ID.2024\_169 PNRR M1C1I1.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU. SERVIZIO DI CONSULENZA E ACQUISTO FORNITURE PER L'ATTUAZIONE DEL PROGETTO "CYBER CMGE"- AFFIDAMENTO IN HOUSE AI SENSI DELL'ART. 7 DEL D.LGS. N. 36/2023 A LIGURIA DIGITALE S.P.A. - CUP D41B20001480006 - CIG B451B6CDF8 - IMPORTO DI EURO 1.257.713,37 ONERI FISCALI INCLUSI." con cui il Responsabile della Direzione Sviluppo economico e provveditorato della Città Metropolitana di Genova ha disposto l'affidamento in house all'operatore economico sopra evidenziato;
- il Contratto di appalto ID.2024\_169 PNRR M1C1I1.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU avente ad oggetto affidamento in house ai sensi dell'art. 7 del D. Lgs. 36/2023 del servizio di consulenza e acquisto forniture per l'attuazione del progetto "CYBER CMGE"- CUP D41B20001480006 - CIG B451B6CDF8;
- la Nota di ACN, assunta agli atti della Città Metropolitana di Genova con Prot. n. 45707/2025, che trasmette la determina Prot. ACN n. 285155 del 23/07/2025 recante la proroga al 31 marzo 2026 del termine di completamento dei progetti e degli adempimenti di rendicontazione previsti dall'Avviso Pubblico n. 08/2024.

#### **PREMESSO CHE**

- la Nota dell'Agenzia per la Cybersicurezza Nazionale (ACN), assunta agli atti della Città Metropolitana di Genova Prot. n. 45707 del 29/07/2025, relativa alla trasmissione della determina prot. ACN n. 285155 del 23/07/2025, recante la proroga al 31 marzo 2026 del termine di completamento dei progetti e degli adempimenti di rendicontazione previsti dall'Avviso Pubblico n. 08/2024, stabilisce la suddetta proroga

senza necessità di invio di istanze individuali di modifica del cronoprogramma da parte dei Soggetti attuatori;

- l'Articolo 1 "Oggetto" del Contratto di appalto ID.2024\_169 PNRR M1C111.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU avente ad oggetto affidamento in house ai sensi dell'art. 7 del D. Lgs. 36/2023 del servizio di consulenza e acquisto forniture per l'attuazione del progetto "CYBER CMGE"- CUP D41B20001480006 - CIG B451B6CDF8 stabilisce che *L'affidatario si impegna all'esecuzione dell'appalto alle condizioni di cui al presente contratto e agli atti a questo allegati o da questo richiamati*;
- l'Articolo 2 "Documenti Contrattuali" del suddetto Contratto stabilisce, tra l'altro, che *"L'appalto viene conferito ed accettato sotto l'osservanza piena, assoluta, inderogabile ed inscindibile delle norme, condizioni, patti, obblighi, oneri e modalità dedotti e risultanti dal Decreto Legislativo 31 marzo 2023, n. 36, degli atti dirigenziali citati in premessa, di tutti i documenti relativi alla procedura di affidamento, che formano parte integrante e sostanziale del presente contratto, ancorché non materialmente allegati"* e che il Capitolato speciale d'appalto forma parte integrante e sostanziale del contratto;
- l'Articolo 9 "Varianti introdotte dal Committente" del Capitolato speciale d'appalto relativo alla fornitura di un servizio di consulenza per attuazione Progetto "CYBER-CMGE" - CUP D41B20001480006 stabilisce che *"La Stazione Appaltante, nei casi previsti dalla normativa vigente, potrà richiedere variazione al contratto stipulato. In tali casi, l'Appaltatore è obbligato ad assoggettarsi alla variazione richiesta alle stesse condizioni previste dal contratto"*;
- L'Articolo 3 "Durata del contratto del contratto d'appalto" è modificato con la modifica contrattuale in data 28/11/2025 come segue: *"La durata del contratto è prorogata e il servizio di supporto alla gestione del progetto dovrà essere integralmente eseguito entro il 31 marzo 2026"*.
- L'Articolo 4 "Corrispettivo del contratto d'appalto" è modificato con la modifica contrattuale in data 28/11/2025 come segue: *"i) L'importo contrattuale per l'esecuzione del servizio ammonta a Euro 1.257.713,37# (unmilione duecentocinquantesette milasettecentotredici/37 euro) oneri fiscali inclusi; ii) Con riferimento alla quota parte dell'importo contrattuale, pari a Euro 650.603,38€ (seicentocinquanta mila seicentotré/38 euro) oneri fiscali inclusi, dedicata all'acquisto di beni e servizi da parte di Liguria Digitale a norma del D.lgs. n. 36/2023 e s.m.i., come risultante dall'atto dirigenziale n. 3011 del 22/11/2024, i ribassi di gara potranno essere utilizzati per ulteriori servizi o forniture funzionali alla realizzazione del progetto su richiesta della Città Metropolitana di Genova, previa modifica contrattuale; iii) L'Affidatario riconosce che il prezzo è remunerativo e di non avere, quindi, alcun diritto a chiedere ulteriori patti, condizioni, prezzi e/o compensi diversi, maggiori o comunque più favorevoli di quelli fissati; iv) L'importo contrattuale è integralmente finanziato con fondi dell'Unione Europea - PNRR NextGenerationEU – Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"*.

La Città Metropolitana di Genova, così come sopra rappresentata, e l'operatore economico Liguria Digitale S.p.A.

TUTTO CIO' PREMESSO

LE PARTI CONVENGONO E STIPULANO QUANTO SEGUE:

**L'Articolo 2 "Documenti contrattuali" è modificato come segue:**

*L'appalto viene conferito ed accettato sotto l'osservanza piena, assoluta, inderogabile ed inscindibile delle norme, condizioni, patti, obblighi, oneri e modalità dedotti e risultanti dal Decreto Legislativo 31 marzo 2023, n. 36, degli atti dirigenziali citati in premessa, di tutti i documenti relativi alla procedura di affidamento, che formano parte integrante e sostanziale del presente contratto, ancorché non materialmente allegati, in particolare:*

- a) *capitolato speciale d'appalto;*
- b) ***modifiche all'articolo 2 e all'articolo 3 del capitolato speciale d'appalto;***
- c) *proposta tecnico economica dell'Affidatario;*
- d) *appendice contrattuale allegata al presente contratto, relativa all'accordo sul trattamento dei dati personali tra il titolare e il responsabile.*

Per la Città Metropolitana di Genova

Dott.ssa Laura Papaleo

Servizio Strategie digitali, ICT  
e finanziamenti europei

Per l'Affidatario

Lorenzo Rizzo e Alessandro Lino

Procuratori Speciali

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

**Missione 1 - Componente 1 - Asse 1**

**Investimento 1.5 “Cybersecurity”**

**PNRR – Missione 1 – Componente 1 – Asse 1**  
**Investimento 1.5 “Cybersecurity”**

**CAPITOLATO SPECIALE DI APPALTO**

**FORNITURA DI UN SERVIZIO DI CONSULENZA PER  
ATTUAZIONE PROGETTO “CYBER-CMGE”**

**CUP D41B20001480006**

**MODIFICA ARTICOLO 2 E ARTICOLO 3**

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

**Missione 1 - Componente 1 - Asse 1**

**Investimento 1.5 "Cybersecurity"**

## **INDICE**

<b>ART. 2 CARATTERISTICHE DEL SERVIZIO .....</b>	<b>3</b>
Intervento 1A: Analisi della postura di sicurezza e definizione di un piano di potenziamento ..	3
Intervento 1B: Miglioramento dei processi e dell'organizzazione .....	3
Intervento 1D: Acquisto e messa in esercizio della piattaforma di asset inventory .....	3
Intervento 2A: Analisi della postura di sicurezza e definizione di un piano di potenziamento ..	4
Intervento 2C: Piattaforma per la diffusione della conoscenza di base relativa alla cyber security awareness.....	4
Intervento 2D: Acquisto e messa in esercizio piattaforma MTM (Mobile Threat Management)	4
Intervento 3C: Consolidamento conoscenza specialistica e conseguimento certificazioni COMPTIA.....	4
Intervento 3D: Progettazione e sviluppo di nuovi sistemi e tecnologie .....	5
Intervento 4C: Consolidamento conoscenza specialistica in ambito Windows Server e Active Directory.....	5
Intervento 5A: Acquisto di apparati attivi necessari alla segmentazione della rete (Layer 3) + WIFI centralizzato.....	6
Intervento 5C: Consolidamento conoscenza specialistica in ambito Microsoft Windows client (Win11) ed in ambito infrastruttura e gestione apparati attivi .....	6
Intervento 5D: Progettazione e sviluppo di nuovi sistemi e tecnologie .....	6
<b>ART. 3 FORNITURE DA ACQUISTARE [<i>Soppresso (inglobato nel ART 2.)</i>].....</b>	<b>7</b>
ITEM_A - Apparati di rete centrali e periferici.....	8
ITEM_B - Sistema wifi centralizzato .....	8
ITEM_C - Piattaforma asset inventory .....	9
ITEM_D – Piattaforma MTM .....	9
ITEM_E – Formazione.....	9

PIANO NAZIONALE DI RIPRESA E RESILIENZA  
Missione 1 - Componente 1 - Asse 1  
Investimento 1.5 "Cybersecurity"

## ART. 2 CARATTERISTICHE DEL SERVIZIO

Il servizio richiesto comprende la fornitura di personale di adeguato livello professionale e di asset tecnologici (fornitura di hardware, licenze, etc) per la realizzazione delle seguenti attività. L'affidamento prevede l'acquisto delle forniture di beni e servizi per assicurare la corretta realizzazione delle attività di progetto. Le forniture di beni devono essere acquistate utilizzando eventuali convenzioni CONSIP attive o, se non presenti, utilizzando il Mercato Elettronico della Pubblica Amministrazione.

### Intervento 1A: Analisi della postura di sicurezza e definizione di un piano di potenziamento

<b>Attività:</b> Analisi dei report, vulnerability assessment e campagne di phishing	<b>N.GIORNI</b>
Account Manager	4
Administration	10
ICT Security Specialist	70
Project Manager	20
<b>TOT</b>	<b>104</b>

### Intervento 1B: Miglioramento dei processi e dell'organizzazione

<b>Attività:</b> Consolidamento dei documenti relativi alla descrizione dell'organizzazione dei processi	<b>N.GIORNI</b>
Account Manager	7
Administration	3,5
Business Analyst	170
Project Manager	27
<b>TOT</b>	<b>207,5</b>

### Intervento 1D: Acquisto e messa in esercizio della piattaforma di asset inventory

<b>ID ITEM</b>	<b>Descrizione</b>	<b>Totale (IVA incl)</b>
<b>ITEM_1D</b>	Piattaforma asset inventory	<b>55.400,00 €</b>

Si considera per questo item, l'acquisto e l'attività di configurazione iniziale (set up) di un sistema di asset inventory per l'Ente.

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

Missione 1 - Componente 1 - Asse 1

Investimento 1.5 "Cybersecurity"

**Intervento 2A: Analisi della postura di sicurezza e definizione di un piano di potenziamento**

<b>Attività:</b> Test di vulnerability assessment della infrastruttura di rete	<b>N.GIORNI</b>
ICT Security Specialist	51
<b>TOT</b>	<b>51</b>

**Intervento 2C: Piattaforma per la diffusione della conoscenza di base relativa alla cyber security awareness**

ID ITEM	Descrizione	Totale (IVA incl.)
<b>ITEM_2C</b>	Corsi di formazione specialistica per la diffusione della conoscenza di base relativa alla cyber security	<b>76.860,00 €</b>

Si considera per questo item, l'acquisto e l'attività organizzazione dei corsi di formazione specifica per il personale tecnico dell'ente e per il personale dei Comuni aderenti al progetto. Nello specifico:

- Corsi base a tema Cyber Security Awareness per fornire ai dipendenti dell'Ente e dei Comuni del Territorio aderenti al progetto, le conoscenze necessarie a fronteggiare il costante evolversi degli attacchi cyber;

**Intervento 2D: Acquisto e messa in esercizio piattaforma MTM (Mobile Threat Management)**

ID ITEM	Descrizione	Totale (IVA incl.)
<b>ITEM_2D</b>	Acquisto e messa in esercizio piattaforma MTM (Mobile threat management)	<b>28.200,00 €</b>

Si considera per questo item, l'acquisto e l'attività di configurazione iniziale (set up) del sistema di Mobile threat management per l'Ente, avente le seguenti caratteristiche minimali.

**Intervento 3C: Consolidamento conoscenza specialistica e conseguimento certificazioni COMPTIA**

ID ITEM	Descrizione	Totale (IVA incl.)
<b>ITEM_3C</b>	Corsi di formazione specialistica e conseguimento certificazioni COMPTIA	<b>83.448,00 €</b>

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

Missione 1 - Componente 1 - Asse 1

Investimento 1.5 "Cybersecurity"

Si considera per questo item, l'acquisto e l'attività organizzazione dei corsi di formazione specifica per il personale tecnico dell'ente e per il personale dei Comuni aderenti al progetto. Nello specifico:

- Corsi specialistici propedeutici alle certificazioni COMPTIA (Security+ e Network+) per il personale tecnico IT degli dell'Ente e dei Comuni del Territorio aderenti al progetto;

**Intervento 3D: Progettazione e sviluppo di nuovi sistemi e tecnologie**

<b>Attività:</b> Acquisto e messa in esercizio servizio SIEM e acquisto/integrazione servizio XDR (per Città Metropolitana di Genova e per i Comuni aderenti al progetto)	<b>N.GIORNI</b>
ICT Security Specialist	75
<b>TOT</b>	<b>75</b>

L'intervento 3D include inoltre, la fornitura evolutiva, attivazione, integrazione, test e messa in esercizio dei sistemi XDR (per l'Ente ed i Comuni metropolitani aderenti al progetto) e SIEM (per la Città Metropolitana di Genova), completati e collaudati entro il 31/03/2026, strumentali al raggiungimento delle milestone di sicurezza cyber previste dall'Investimento 1.5 del PNRR come indicato nella tabella che segue:

ID ITEM	Descrizione	Totale (IVA incl.)
<b>ITEM_3D</b>	fornitura evolutiva, attivazione, integrazione, test e messa in esercizio dei sistemi XDR (per l'Ente ed i Comuni metropolitani aderenti al progetto) e SIEM (per la Città Metropolitana di Genova).	<b>217.312,27 €</b>

La fornitura include e assicura la disponibilità tecnica delle licenze e delle console con scadenza al 31/05/2029, quale naturale estensione temporale dell'asset tecnologico attivato e collaudato entro la scadenza PNRR.

**Intervento 4C: Consolidamento conoscenza specialistica in ambito Windows Server e Active Directory**

ID ITEM	Descrizione	Totale (IVA incl.)
<b>ITEM_4C</b>	Consolidamento conoscenza specialistica in ambito Windows Server e Active Directory	<b>27.694,00 €</b>

Si considera per questo item, l'acquisto e l'attività organizzazione dei corsi di formazione specifica per il personale tecnico dell'ente e per il personale dei Comuni aderenti al progetto. Nello specifico:

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

Missione 1 - Componente 1 - Asse 1

Investimento 1.5 "Cybersecurity"

- Corsi specialistici in ambito Windows Server relativi al miglioramento delle competenze riguardanti la progettazione, l'implementazione, la configurazione e la gestione di un ambiente Microsoft Active Directory;

**Intervento 5A: Acquisto di apparati attivi necessari alla segmentazione della rete (Layer 3) + WIFI centralizzato**

ID ITEM	Descrizione	Totale (IVA incl.)
ITEM_5A	Apparati di rete centrali e periferici della rete informatica di CMGE	<b>287.835,87 €</b>

**Apparati di rete centrali e periferici**

Si considera per questo item l'acquisto per la sostituzione di tutti gli apparati di rete dell'Ente (Layer 3) e Sistema WiFi centralizzato.

**Intervento 5C: Consolidamento conoscenza specialistica in ambito Microsoft Windows client (Win11) ed in ambito infrastruttura e gestione apparati attivi**

ID ITEM	Descrizione	Totale (IVA incl.)
ITEM_5C1	Consolidamento conoscenza specialistica in ambito Microsoft Windows client (Win11)	<b>36.600,00 €</b>
ITEM_5C2	Consolidamento conoscenza specialistica e certificazione in ambito infrastruttura e gestione apparati attivi	<b>18.118,46 €</b>

Si considera per questo item, l'acquisto e l'attività organizzazione dei corsi di formazione specifica per il personale tecnico dell'ente e per il personale dei Comuni aderenti al progetto. Nello specifico:

- Corsi specialistici in ambito Windows 11 relativi al miglioramento delle competenze riguardanti la gestione del client di Windows;
- Corsi di formazione specialistica e certificazione sui prodotti di rete acquistati per il rafforzamento della infrastruttura di rete dell'ente

**Intervento 5D: Progettazione e sviluppo di nuovi sistemi e tecnologie**

<b>Attività:</b> Acquisto e messa in esercizio servizio di Lan Monitoring and Management	<b>N.GIORNI</b>
Account Manager	3
Administration	2

PIANO NAZIONALE DI RIPRESA E RESILIENZA  
Missione 1 - Componente 1 - Asse 1  
Investimento 1.5 "Cybersecurity"

Network and System Specialist	53
Service Manager	32
Project Manager	20
<b>TOT</b>	<b>110</b>

L'intervento 5D include inoltre, la fornitura evolutiva, attivazione, integrazione, test e messa in esercizio del sistema PRTG (per l'Ente), completati e collaudati entro il 31/03/2026, strumentali al raggiungimento delle milestone di sicurezza cyber previste dall'Investimento 1.5 del PNRR come indicato nella tabella che segue:

ID ITEM	Descrizione	Totale (IVA incl.)
<b>ITEM_5D</b>	fornitura evolutiva, attivazione, integrazione, test e messa in esercizio del sistema PRTG (per l'Ente) in modalità "enterprise" circa 2500 sensori.	<b>136.559,65 €</b>

La fornitura include e assicura la disponibilità tecnica delle licenze e delle console con scadenza al 31/05/2029, quale naturale estensione temporale dell'asset tecnologico attivato e collaudato entro la scadenza PNRR.

### ART. 3 **FORNITURE DA ACQUISTARE [Soppresso (inglobato nel ART 2.)]**

L'affidamento in oggetto prevede l'acquisto delle forniture di beni e servizi sotto elencati. Le forniture di beni devono essere acquistate utilizzando eventuali convenzioni CONSIP attive o, se non presenti, utilizzando il Mercato Elettronico della Pubblica Amministrazione.

Per ciascuna fornitura è richiesto di specificare il dettaglio dei costi.

ID ITEM	Descrizione	Totale a disposizione (IVA esclusa)
<b>ITEM_A</b>	Apparati di rete centrali e periferici della rete informatica di CMGE	<b>408.500,00 €</b>
<b>ITEM_B</b>	Sistema wifi centralizzato interconnesso alla rete informatica di CMGE	<b>89.131,15 €</b>
<b>ITEM_C</b>	Piattaforma asset inventory	<b>45.409,84 €</b>

PIANO NAZIONALE DI RIPRESA E RESILIENZA

Missione 1 - Componente 1 - Asse 1

Investimento 1.5 "Cybersecurity"

ITEM_D	Acquisto e messa in esercizio piattaforma MTM (Mobile threat management)	23.114,75 €
ITEM_E	Corsi di formazione specifica	152.590,00 €

### ITEM\_A - Apparati di rete centrali e periferici

Si considera per questo item l'acquisto per la sostituzione di tutti gli apparati di rete dell'Ente, così suddiviso:

- n. 2 switch 24 porte in fibra ottica layer 3
- n. 50 switch 48 porte PoE layer 3
- n. 36 gruppi di continuità da rack dimensionati per switch sopra indicati
- Patch cord e accessori armadi rack necessari all'installazione
- Software di gestione centralizzato

All'interno della cifra indicata sono considerati anche i costi per attività di acquisto, sopralluogo tecnico iniziale, lavori di posa in opera, configurazione degli apparati e collaudo finale.

### ITEM\_B - Sistema wifi centralizzato

Si considera per questo item, l'acquisto dei dispositivi wifi per l'intera copertura wireless della sede distaccata di Quarto (Largo Cattanei 3 – Genova). Nello specifico sono richiesti:

- n. 60 Access Point con le seguenti caratteristiche minimali:
  - IEEE 802.11ax (Wifi6 certified)
  - possibilità di realizzare un sistema di distribuzione wireless WDS ovvero possibilità di utilizzare il mezzo radio Wi-fi per la distribuzione della connettività "backhaul" verso Access Point non direttamente connessi alla rete cablata contemporaneamente alla funzione di AP. I dispositivi offerti dovranno pertanto garantire contemporaneamente la funzione di AP e di WDS.
  - almeno una interfaccia base T con supporto del protocollo IEEE 802.3bz
  - Client Authentication alle WLAN tramite captive portal con repository utenze interno ed esterno
  - capacità di localizzazione e gestione dei rogue access point
- Cablaggio dei relativi punti rete necessari
- Patch cord e accessori armadi rack necessari all'installazione
- Software di gestione centralizzato

**Il Brand per gli Access Point forniti deve essere lo stesso del Brand degli Switch**

PIANO NAZIONALE DI RIPRESA E RESILIENZA

Missione 1 - Componente 1 - Asse 1

Investimento 1.5 "Cybersecurity"

All'interno della cifra indicata sono considerati anche i costi per attività di acquisto, sopralluogo tecnico iniziale, lavori di posa in opera, configurazione degli apparati e collaudo finale.

### **ITEM\_C - Piattaforma asset inventory**

Si considera per questo item, l'acquisto e l'attività di configurazione iniziale (set up) di un sistema di asset inventory per l'Ente, avente le seguenti caratteristiche minimali:

open source, interfaccia web based, storia completa delle modifiche effettuate su qualunque scheda dati (versioning), funzioni di ricerca avanzata, definizione di filtri e viste per un accesso personalizzato ai dati, associazione di documenti alla singola scheda, motore di workflow integrato per gestione flussi ticket, reportistica integrata, profilazione utenti/gruppi di utenti con modalità multitenant, interoperabilità con altre applicazioni tramite webservice in particolare con l'infrastruttura Active Directory e con il sistema OCS Inventory presenti nell'Ente, funzioni di import / export CSV, possibilità di configurare e gestire operazioni automatiche (compreso invio mail), fornitura di un Portale Self-Service per gli utenti non tecnici, fornitura di APP mobile per gestione ticket.

### **ITEM\_D – Piattaforma MTM**

Si considera per questo item, l'acquisto e l'attività di configurazione iniziale (set up) del sistema di Mobile threat management per l'Ente, avente le seguenti caratteristiche minimali:

gestione centralizzata dei dispositivi mobili, monitoraggio dei dispositivi mobili in ottemperanza alle normative sulla privacy, protezione della connettività internet dei dispositivi mobili con particolare attenzione ai casi di contatti o connessioni con reti di tipo wifi esterne all'Ente, protezione nell'utilizzo di applicazioni di posta elettronica, messaggistica e navigazione web contro malware, phishing e smishing, protezione di dati e documenti che si trovano sui dispositivi mobili, report di sicurezza degli eventi potenzialmente pericolosi e degli attacchi verificatisi, assistenza per il mantenimento aggiornato delle APP presenti sui dispositivi e l'individuazione di possibili di loro vulnerabilità legate a versioni superate.

### **ITEM\_E – Formazione**

Si considera per questo item, l'acquisto e l'attività organizzazione dei corsi di formazione specifica per il personale tecnico dell'ente e per il personale dei Comuni aderenti al progetto. Nello specifico:

- Corsi base a tema Cyber Security Awareness per fornire ai dipendenti dell'Ente e dei Comuni del Territorio aderenti al progetto, le conoscenze necessarie a fronteggiare il costante evolversi degli attacchi cyber;
- Corsi specialistici propedeutici alle certificazioni COMPTIA (Security+ e Network+) per il personale tecnico IT degli dell'Ente e dei Comuni del Territorio aderenti al progetto;

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

**Missione 1 - Componente 1 - Asse 1**

**Investimento 1.5 “Cybersecurity”**

- Corsi specialistici in ambito Windows Server relativi al miglioramento delle competenze riguardanti la progettazione, l'implementazione, la configurazione e la gestione di un ambiente Microsoft Active Directory.
- Corsi di formazione specialistica e certificazione sui prodotti di rete acquistati per il rafforzamento della infrastruttura di rete dell'ente.