AGENZIA REGIONALE PROTEZIONE AMBIENTALE DELLA CAMPANIA

DELIBERAZIONE DEL DIRETTORE GENERALE N. 584 DEL 26/11/2024

IL RUP LA VIA

OGGETTO: AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006_ADESIONE AQ ID 2296, LOTTO 2 "SERVIZI DI COMPLIANCE E CONTROLLO". CIG B457DB055E.

L'anno duemilaventiquattro, il giorno ventisei del mese di Novembre presso la sede dell'A.R.P.A.C. alla stregua dell'istruttoria compiuta dal RUP e della dichiarazione di completezza e regolarità resa dal medesimo

PREMESSO CHE:

- con deliberazione n. 532 del 14.11.2018 l'ARPAC ha nominato il Responsabile per la Transizione al Digitale, ai sensi dell'articolo 17, del rinnovato decreto legislativo 82/2005 (Codice dell'Amministrazione Digitale), individuandolo nella dott.ssa Loredana La Via, dirigente della UO Sistemi Informativi e Informatici, cui sono affidati i compiti di conduzione del processo di transizione alla modalità operativa digitale e dei conseguenti processi di riorganizzazione, finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
- tra i compiti affidati al RTD rientra quello inerente indirizzo, pianificazione, coordinamento e monitoraggio della *sicurezza informatica* relativamente ai dati, ai sistemi ed alle infrastrutture, anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, c. 1 del citato CAD;
- il tema della cybersicurezza è quando mai attuale e fortemente attenzionato anche a livello UE;
- la nuova direttiva europea NIS 2 (Direttiva n. 2022/2555, entrata in vigore il 17 gennaio 2023 << … *relativa a misure per un livello comune elevato di cybersicurezza nell'Unione,….* > che abroga la precedente Direttiva (UE) 2016/1148 - "Direttiva NIS 1" - recepita in Italia attraverso il D. Lgs. n. 65/2018 e da cui di fatto la nuova NIS 2 prende forma e sostanza) che introduce, tra l'altro, misure più stringenti e specifiche in termini di cyber risk management e di segnalazione e *condivisione* delle informazioni relative agli incidenti di sicurezza, è in vigore in Italia a partire dal 16.10.2024, a seguito del D. Lgs. n. 138 del 04.09.2024;
- secondo l'Osservatorio Cybersecurity & Data Protection la protezione contro i rischi di tipo cyber sta diventando sempre più una priorità di investimento in Italia, con il 67% delle imprese italiane ad aver segnalato un incremento dei casi di attacchi malevoli;
- con determina ACN prot. n. 5959 del 26 febbraio 2024 recante «Avviso Pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul Piano Nazionale di Ripresa e

Resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” – Codice d’investimento M1C1I1.5», sono stati approvati gli atti costituenti l’Avviso 08/2024, tra cui l’allegato C “Atto d’Obbligo”, e relativa pubblicazione;

- con nota prot. n. 23488 del 12.04.2024 l’Agenzia ha presentato domanda di partecipazione all’Avviso pubblico ACN n. 8/2024 di cui sopra;
- con determina ACN prot. n. 22329 del 09/07/2024 recante «Avviso Pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell’ambiente a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” – Codice d’investimento M1C1I1.5. Determina di ammissione ed esclusione delle domande pervenute e nomina della Commissione di valutazione», è stata nominata la Commissione di valutazione e sono state ammesse al prosieguo della valutazione n. 94 proposte progettuali;
- con determina ACN prot. n. 30550 del 23.09.2024 è stato approvato l’aggiornamento degli elenchi predisposti dalla Commissione di valutazione e, conseguentemente, la graduatoria definitiva a valere sull’Avviso 8/2024, di cui costituisce parte integrante e sostanziale l’Allegato A **“**Graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili” in cui risulta presente la proposta di progetto di ARPA Campania, ammesso a finanziamento per l’intero importo richiesto, ossia € 1.262.713,42 IVA inclusa;
- con deliberazione n. 512 del 17.10.2024 l’Ente prende atto dell’ammissione al finanziamento di cui sopra;
- con nota prot. n. 65945 del 25.10.2024 l’Ente ha trasmesso l’Atto d’obbligo, ai sensi dell’art. 10 dell’Avviso ACN n. 8/2024;
- il progetto in questione si pone l’obiettivo di migliorare la postura cyber dell’Ente, con un articolato piano strategico, avvalendosi di una attività di assessment e potenziamento della resilienza cyber e rafforzandosi così in termini di compliance e formazione;
- per fare ciò occorre perseguire la roadmap di iniziative che prevedono di identificare lo stato di esposizione alle vulnerabilità, gestire gli eventuali incidenti di sicurezza, eseguire attacchi simulati per sfruttare le vulnerabilità e, di conseguenza, prenderne le dovute protezioni, e migliorare la compliance normativa;
- tali obiettivi del progetto ARPAC sono raggiungibili mediante oculata adesione all’Accordo Quadro CONSIP per *<<l’Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni” – ID2296, Lotto 2 “Servizi di compliance e controllo”>>* che prevede articolati servizi, tra cui sono stati scelti i seguenti:
  - L2.S16: Security Strategy - per individuare le azioni appropriate per gestire i rischi di sicurezza;
  - L2.S17: Vulnerability Assessment - per identificare le vulnerabilità presenti nella rete ARPAC;
  - L2.S21: Supporto all’analisi e gestione degli incidenti - per consulenze volte ad incrementare l’efficacia e l’efficienza dei processi di Forensic e Incident Management;

- L2.S22: Penetration Testing - per verificare, con degli attacchi simulati, la possibilità di sfruttare eventuali vulnerabilità identificate nella rete ARPAC;
- L2.S23: Compliance Normativa - per gestire al meglio tutti gli adempimenti GDPR;

- con nota prot. n. 67993/2024 del 31.10.2024 l'Ente ha trasmesso all'ACN l'avvio delle attività e le modifiche al progetto finanziato relativamente al cronoprogramma, atto dovuto essendo trascorsi svariati mesi prima dell'esito della valutazione da parte della Commissione ACN;
- con deliberazione n. 566 del 14.11.2024 l'Ente ha aderito all'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296 – Lotto 1 "Servizi di Sicurezza da Remoto"* per l'acquisizione, per l'annualità 2025, di beni e tecnologie inerenti una prima tranche del finanziamento PNRR in questione;

CONSIDERATO CHE

- il Piano dei Fabbisogni, contenente le indicazioni sulla tipologia dei servizi necessari all'Agenzia per il raggiungimento degli obiettivi di progetto, il loro dimensionamento e le quantità richieste, è stato trasmesso al Fornitore in data 12.11.2024 con nota prot. n. 70412/2024;
- il RTI Fornitore ha predisposto e trasmesso all'Agenzia, in data 18.11.2024 con prot. n. 71773/2024, il 'Piano Operativo' esplicativo dei servizi richiesti corredati dei costi ottenuti applicando i prezzi unitari di cui all'Accordo Quadro;
- come da progetto ARPAC ammesso al finanziamento PNRR, i servizi in Accordo Quadro ID 2296, Lotto 2, sono coperti tramite i fondi inerenti l'Avviso ACN n. 8/2024 relativi a Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5;
- l'Accordo Quadro recita che il 'Piano dei Fabbisogni' potrà essere variato e/o aggiornato dall'Amministrazione ogni qualvolta questa lo ritenga necessario;
- il RTI Fornitore dovrà di conseguenza, in tali eventualità, aggiornare il 'Piano Operativo' nei tempi e modi come da Contratto;

RITENUTO CHE

- l'Agenzia, in quanto Pubblica Amministrazione, rimane soggetta a tutto quanto disposto dalla Circolare AgID n. 2/2017, recante *"Misure minime di sicurezza ICT per le pubbliche amministrazioni"* ed alla Direttiva NIS2, pertanto al D. Lgs. n. 138 del 04.09.2024;
- con il progetto ammesso a finanziamento con fondi PNRR ARPAC ha l'opportunità di identificare lo stato di salute della sicurezza del sistema informativo dell'Ente al fine di garantire la corretta postura cyber, sulla base della roadmap delle attività da svolgere e colmare, così, le probabili vulnerabilità presenti nello stesso;
- il Piano Operativo, prot. n. 71773/2024 del 18.11.2024 inviato dal RTI Fornitore, sia adeguato da un punto di vista prestazionale andando a soddisfare pienamente le esigenze agenziali come sopra specificate;

- si debba procedere, pertanto, all'approvazione dello schema di "Contratto Esecutivo" e del nuovo "Piano Operativo";

ATTESO CHE tutti gli atti richiamati nella presente deliberazione sono depositati presso l'ufficio proponente;

VISTI

- il Regolamento Europeo sulla Protezione dei Dati (UE 679/2016);
- la Direttiva NIS2 – Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14.12.2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972;
- il D. Lgs. 36/2023;
- il D. Lgs. n. 138 del 04.09.2024;
- la Determina di ACN di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse con aggiornamento del circuito finanziario – n. protocollo 30550 del 23.09.2024;
- la Circolare AgID n. 2/2017, recante *"Misure minime di sicurezza ICT per le pubbliche amministrazioni";*
- la L. R. 10/98 ed il vigente Regolamento sull'Organizzazione di ARPAC;
- la deliberazione n. 760/2023 di approvazione di Bilancio di previsione esercizio 2024 e pluriennale per il triennio 2024/2026;

Per tutto quanto premesso e considerato si propone di adottare la seguente

DELIBERAZIONE

Per le motivazioni espresse in narrativa che qui si intendono integralmente riportate e trascritte:

- di aderire all'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296 – Lotto 2 "Servizi di Compliance e Controllo"*, per un periodo pari a n. 13 mesi (01.12.2024 – 31.12.2025) per l'acquisizione dei seguenti servizi opportunamente dimensionati, come da Piano Operativo:
  - L2.S16: Security Strategy
  - L2.S17: Vulnerability assessement
  - L2.S21: Supporto all'analisi e gestione degli incidenti
  - L2.S22: Penetration testing
  - L2.S23: Compliance normativa;

- di individuare il RTI composto da
  - *Deloitte Risk Advisory S.r.L.*
  - *EY Advisory S.p.A.*
  - *Teleco S.r.L.*

come Fornitore per la realizzazione esecutiva delle esigenze agenziali in materia di Cybersicurezza come su delineate;

- di approvare lo "Schema di Contratto esecutivo" per la fornitura dei servizi di sicurezza di cui al Lotto 2 dell'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296 – Lotto 2* che, allegato alla presente, ne costituisce parte integrante e sostanziale;
- di approvare l'allegato "Piano Operativo", comprensivo dei canoni e dell'utilizzo di figure professionali 'a consumo' per la fornitura, per un periodo di 13 mesi, dei servizi di seguito dettagliati:
  - L2.S16: Security Strategy
  - L2.S17: Vulnerability assessement
  - L2.S21: Supporto all'analisi e gestione degli incidenti
  - L2.S22: Penetration testing
  - L2.S23: Compliance normativa;
- di precisare che la presente fornitura, nel periodo 01.12.2024 – 31.12.2025, è pagabile con finanziamento PNRR - Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5" di cui sopra, per un totale pari ad € 807.300,00 (IVA esclusa);
- di puntualizzare, inoltre, che la somma di € 984.906,00 (IVA compresa) è stata impegnata con impegno n. 534/2024 – Capitolo 10563, esercizio 2024;
- di precisare altresì che la somma di € 984.906,00 è stata accertata con accertamento n. 166/2024 – Capitolo 61128, esercizio 2024;
- di impegnare sul Capitolo n. 10502 "Utenze" del Bilancio di competenza 2024 e pagare, ai sensi dell'art. 4, c. 3-quater, del D. L. 6 luglio 2012, n. 95, convertito con modificazioni in L. 7 agosto 2012, n. 135, il contributo di cui all'art. 18, c. 3, D. Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010, a favore di CONSIP SpA nella misura dell'8 per mille del valore del contratto esecutivo, pari pertanto ad € 6.458,40, da pagare tramite bonifico bancario specificando nella causale "Accordo Quadro per l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – ID2296 – Lotto 2";
- di dare atto che gli impegni di spesa di cui sopra sono soggetti alle disposizioni di cui all'art. 56 del D. Lgs. 118/2011;
- di affidare alla UO Sistemi Informativi e Informatici la verifica della regolarità del servizio nonché, a seguito di parere favorevole, l'autorizzazione della proposta di liquidazione trasmessa dall'U.O Bilancio Contabilità e Finanze, previa acquisizione del DURC;
- di precisare che la presente fornitura, per tipologia di prestazione, non è classificabile secondo il Catalogo dei servizi SNPA in quanto trattasi di spesa a carattere generale;

- di demandare alla UO AGCO di procedere con la sottoscrizione del contratto, il cui schema è approvato con la presente deliberazione, e con il relativo repertorio;
- di disporre, ai sensi dell'art. 3 della L. 136/2010 che tutti i pagamenti a favore del "*RTI Fornitore*" relativi al presente affidamento debbano essere eseguiti tramite conto corrente dedicato di cui al comma 1 dell'art. 3 della Legge n. 136/2010 e mediante bonifico bancario o postale ovvero altri strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni;
- di nominare quale Direttore dell'Esecuzione il dott. Di Guida Massimo, attese le competenze in materia.

Napoli, 19 novembre 2024

Il RUP

Dott.ssa Loredana La Via

La proposta di deliberazione è accolta.

Napoli, 26/11/2024

Il Direttore Generale
Avv. Luigi Stefano SORVINO

OGGETTO: AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006_ADESIONE AQ ID 2296, LOTTO 2 "SERVIZI DI COMPLIANCE E CONTROLLO". CIG B457DB055E.

PARERE DI REGOLARITA' AMMINISTRATIVA

Sulla suesposta proposta, avente ad oggetto "AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006_ADESIONE AQ ID 2296, LOTTO 2 "SERVIZI DI COMPLIANCE E CONTROLLO". CIG B457DB055E.", in ordine alla regolarità amministrativo-contabile ed alla copertura finanziaria, si esprime parere favorevole.

Data **26/11/2024**

Il Direttore Amministrativo a.i.

Luca Antonio Esposito / InfoCert S.p.A.

DELIBERAZIONE N° 584 DEL 26/11/2024

ATTESTAZIONE DI PUBBLICAZIONE

Si dichiara che la presente deliberazione è stata affissa all'Albo di questa Agenzia dal giorno 26/11/2024 e vi resterà per gg 15 (quindici) .

Napoli, **26/11/2024**

Il Funzionario Incaricato
Valeria Torella / INFOCERT SPA

DELIBERAZIONE N° 584 DEL 26/11/2024

ATTESTAZIONE DI IMMEDIATA ESEGUIBILITA'

La presente Deliberazione è stata dichiarata immediatamente eseguibile per l'urgenza

Napoli data **26/11/2024**

Il Direttore Generale
Avv. Luigi Stefano SORVINO

Luigi Stefano Sorvino / InfoCert S.p.A.

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Identificativo: Piano Operativo V1

Data: 13/11/2024

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

Piano Operativo

Agenzia Regionale per la Protezione dell'Ambiente della Campania

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Firma

Deloitte. EY teleco

1 INTRODUZIONE

1.1 Ambito

Nel Settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per "l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296". Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Risk Advisory S.r.l. e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell'Accordo Quadro è di 24 mesi, decorrenti dalla data di attivazione. Per durata dell'Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell'Accordo Quadro per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il "Piano Operativo" nel quale l'RTI intende formulare la proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro, in risposta al "Piano dei Fabbisogni" redatto dall'Agenzia Regionale per la Protezione dell'Ambiente della Campania.

1.2 Richieste dell'Amministrazione contraente

L'Agenzia Regionale per la Protezione dell'Ambiente della Campania (di seguito "**ARPAC**"), Ente strumentale della Regione Campania, si compone di un'organizzazione "a rete" con struttura centrale e cinque dipartimenti nelle province di Avellino, Benevento, Caserta, Napoli e Salerno. La struttura centrale (Direzione generale, Direzione tecnica e Direzione amministrativa) definisce le politiche di indirizzo e di sviluppo, coordina le attività tecnico-scientifiche e amministrative dell'ente e ne elabora le strategie di comunicazione**. La diversificazione dei Servizi ai cittadini e alle imprese, la complessità dei servizi offerti e la peculiarità dell'infrastruttura digitale e sistemica adottata dall'ente rilevano quali punti d'attenzione importante,** nella prospettiva di una valutazione realistica della situazione relativa alla cybersecurity, sia tecnica che legata alla consapevolezza del personale e all'indirizzamento di azioni di rimedio, al fine di innalzare la postura complessiva della sicurezza delle informazioni e dei sistemi.

La costante **richiesta di innovazione nel fornire i servizi ai cittadini** e la capacità di dover **rispondere in maniera rapida ed efficace ai cambiamenti imposti anche dall'ambiente esterno** pongono la necessità di una maggior attenzione alle tematiche che riguardano la **sicurezza delle informazioni** e la **protezione dei dati**. Inoltre, l'utilizzo di tecnologie digitali in ogni singolo aspetto produttivo e sociale ha inevitabilmente posto la sicurezza dei sistemi digitali (e delle informazioni che in essi vengono generate, usate, conservate e scambiate) ai primi posti fra le questioni da affrontare per garantire la resilienza dei servizi erogati al cittadino e dell'ecosistema digitale di ARPAC.

Non da ultimo, occorre tener presente che l'Ente ha partecipato e ottenuto il finanziamento relativamente al progetto **"Assessment e potenziamento della resilienza cyber di ARPAC"** in risposta all'Avviso 8/2024 adottato dall'Agenzia per la Cybersicurezza Nazionale (determina n. ACN.AOO_ACN-US.REGISTRO UNICO.0005959del 26 febbraio 2024 con la quale è stato approvato l'Avviso Pubblico, avente ad oggetto *"Avviso Pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere*

sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5").

A tal fine, avvalendosi del finanziamento in oggetto, un **Progetto di Assessment e potenziamento della resilienza cyber**, diviene condizione imprescindibile per garantire la protezione di tutto l'ecosistema coinvolto. L'obiettivo è quello di rafforzare il governo e la maturità di Sicurezza di ARPAC, ossia garantire riservatezza, integrità e disponibilità del patrimonio informativo, nel contesto della digitalizzazione dei servizi dell'Organizzazione.

Anche alla luce delle attuali criticità riscontrate sui sistemi informativi, l'obiettivo principale di ARPAC consta nel predisporre un **Piano strategico** e una **Roadmap evolutiva delle iniziative** in ambito **Cybersecurity** che l'Ente dovrà avviare al fine di irrobustire la propria **Cyber Security Posture,** recependo, inoltre, le risultanze di un assessment che verrà condotto al fine di evidenziare i principali gap sulla cybersecurity, nonché le ulteriori iniziative di sviluppo tecnologico e trasformazione digitale attualmente intraprese dall'Ente.

Allo scopo di innovare i servizi ed incrementare la produttività di ARPAC, la **Sicurezza delle informazioni** rappresenta il principale elemento abilitante al raggiungimento di tale obiettivo.

In quest'ottica, l'eccellenza è il risultato che può essere raggiunto sia migliorando quanto già in essere, sia innovando, al fine di erogare e offrire nuovi servizi. Inoltre, tali risultati possono essere raggiunti attuando un adeguato processo di monitoraggio, misurazione e comunicazione della sicurezza delle informazioni.

Questo modello richiede e prevede l'adozione di un approccio che contempli elementi di novità rispetto al passato così da rispondere alle mutate esigenze di contesto. Inoltre, le sfide a cui si è chiamati a rispondere richiedono l'adozione di una visione strategica di lungo periodo e la definizione di piani tattici con risultati a medio-breve termine.

In linea con quanto sopra descritto, sono stati individuati, nell'ambito del **Lotto 2- Servizi di Compliance e controllo** dell'Accordo Quadro - avente ad oggetto per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni - i seguenti obiettivi di sintesi, anche alla luce delle criticità emerse, che rientrano nel più ampio programma di attuazione del Progetto di analisi dello stato attuale ed evoluzione della postura di sicurezza informatica:

- **Obiettivo 1:** stabilire il livello di maturità dell'Ente e predisporre una roadmap di iniziative (e la relativa attività di follow-up) volte al consolidamento della stessa maturità dell'Ente, in relazione ai risultati emersi e al livello di maturità futuro atteso. L'obiettivo è perseguito anche mediante l'esecuzione di una serie di azioni finalizzate a mitigare i rischi inerenti all'organizzazione e ai servizi erogati, così come per contrastare eventi di cybercrime (L2.S16);
- **Obiettivo 2:** identificare lo stato di esposizione alle vulnerabilità (vulnerability assessment e correlate *Run* di follow-up nell'arco del successivo biennio) mediante la raccolta di informazioni concernente i servizi erogati, le applicazioni, l'architettura e le componenti tecnologiche (L2.S17);
- **Obiettivo 3:** migliorare la gestione degli incidenti per incrementare efficacia ed efficienza dei processi di Incident Management (L2.S21);
- **Obiettivo 4:** eseguire, nell'arco del periodo progettuale, attacchi simulati (Penetration Test) per verificare concretamente la possibilità di sfruttare vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi (L2.S22);
- **Obiettivo 5:** migliorare la compliance normativa in ambito privacy al fine di garantire la piena conformità alla normativa vigente nonché per consentire all'Ente di tutelare i dati personali da esso trattati in qualità di Titolare del Trattamento e di garantire elevati standard di sicurezza degli stessi (L2.S23).

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Allegato 2B - Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Capitolato Oneri	Capitolato d'Oneri della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Bando GURI	Bando GURI della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

1.4 Acronimi e glossario

DEFINIZIONE/ACRONNIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale
PA	Pubblica Amministrazione

PAC	Pubblica Amministrazione Centrale
S.I.	Sistema Informativo
AGID	Agenzia per l'Italia Digitale
ICT	Information and Communications Technology
DLT R.A.	Deloitte Risk Advisory Srl
EY	EY Advisory SpA
Teleco	Teleco Srl

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Agenzia Regionale per la Protezione dell'Ambiente della Campania
Indirizzo	Via Vicinale Santa Maria del Pianto (c. Polifunzionale Torre 1)
CAP	80143
Comune	Napoli
Provincia	NA
Regione	Campania
Codice Fiscale	07407530638
Indirizzo mail	segreteria@arpacampania.it
PEC	direzionegenerale.arpac@pec.arpacampania.it
Codice PA	arlpa_
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Loredana
Cognome	La Via
Telefono	0812326362
Indirizzo mail	l.lavia@arpacampania.it
PEC	

3 CATEGORIZZAZIONE DELL'INTERVENTO

3.1 Categorizzazione di I livello

	AMBITO I LIVELLO (LAYER)	OBIETTIVI PIANO TRIENNALE
	SERVIZI	Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
	DATI	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
		Aumentare la qualità dei dati e dei metadati
		Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
	PIATTAFORME	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
		Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
		Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
		Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
		Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
		Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
	INTEROPERABILITÀ	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
		Adottare API conformi al Modello di Interoperabilità
X	SICUREZZA INFORMATICA	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
		Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

3.2 Categorizzazione di II livello

I LIVELLO (LAYER)		II LIVELLO
SERVIZI		Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
PIATTAFORME		Sanità digitale (FSE e CUP)
		Identità Digitale
		Pagamenti digitali
		App IO
		ANPR
		NoiPA
		INAD
		Musei
		Siope+
DATI		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INTEROPERABILITA		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INFRASTRUTTURE		Data center e Cloud
		Connettività
SICUREZZA INFORMATICA	X	Portali istituzionali e CMS
	X	Sensibilizzazione del rischio cyber

4 Servizi richiesti e ambito di intervento

4.1 Ambiti di intervento

L'ambito funzionale di intervento per tale fornitura è da intendersi finalizzato alla definizione e implementazione di un Piano di potenziamento per la Cybersecurity, con l'**obiettivo di rafforzare il governo e la maturità di Sicurezza del proprio ecosistema**, ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo, nel contesto della digitalizzazione dei servizi dello stesso.

A valle delle attività sopra citate, verranno svolte una serie di attività di follow-up finalizzate alla verifica costante dei risultati raggiunti, anche avvalendosi di un servizio di Project Management e supporto specialistico (PMO).

Lo svolgimento di un assessment sulla postura cyber dell'Ente, per cui saranno tenute in considerazione sia l'eterogeneità delle realtà coinvolte che eventuali e recenti attività di assessment già condotti, è finalizzato a **stabilire il livello di maturità dell'ente e a predisporre una roadmap di iniziative** volte al consolidamento della stessa maturità dell'ente, in relazione ai risultati emersi e al livello di maturità futuro atteso.

Nello specifico, l'assessment verrà condotto su **due livelli** (coinvolgendo, a tal proposito, sia i servizi di Security Strategy che di VA/PT messi a disposizione dal presente Accordo Quadro), ossia:

- **Cyber posture assessment:** sarà condotto sulla base del "Framework Nazionale per la Cyber Security e la Data Protection" e sarà volto ad integrare eventuali attività di assessment precedentemente condotte con focus sulla gestione dei principali processi in ambito sicurezza delle informazioni. Inoltre, verrà condotto uno specifico **Assessment verticale sulla gestione delle identità digitali e degli accessi logici,** atto a definire l'attuale livello di maturità sulle modalità di gestione delle utenze e verranno definiti i **processi operativi** atti a disciplinare la gestione del ciclo di vita delle utenze sopra citate. Da ultimo, in ottica di maggior capillarità, verranno svolti anche degli **assessment verticali sui singoli Dipartimenti** territoriali, facenti parte dell'organizzazione regionale di ARPAC. Attività di formazione come dettagliato successivamente;
- **Cyber Testing:** Esecuzione di Vulnerability Assessment e Penetration Test su un perimetro selezionato di sistemi IT dell'Ente, a seguito della definizione di un piano di test cadenzato e che tenga conto della criticità dei sistemi. L'attività comprenderà il supporto all'organizzazione del piano di rimedio delle vulnerabilità che emergeranno

Al termine dell'assessment verrà adottata una **Roadmap delle iniziative tattiche**, sulla base dei principali standard e leading practices riconosciute in ambito Security ICT (es. ISO27001-2, Linee guida ENISA) come il **Framework Nazionale per la Cybersecurity e la Data Protection (FNCDP).** l'Ente sarà in grado di recepire gli indirizzi strategici e gli input esogeni/endogeni per definire, attraverso l'ausilio di metodologie, approcci operativi e strumenti, il proprio **Piano strategico delle iniziative di Cybersecurity.**

Indipendentemente dall'assessment, verranno parallelamente avviate alcune iniziative di centrale importanza al fine di **mitigare i rischi** inerenti all'organizzazione e ai servizi erogati, così come per contrastare eventi di cybercrime. Le azioni, identificate e customizzate sulla base dell'**eterogeneità** della realtà dell'Ente nonché in linea con le principali normative e standard in ambito Sicurezza (es. ISO27001-2), contribuiranno a **migliorare** complessivamente non solo la **postura di sicurezza dell'Ente** ma anche **il livello di protezione dei dati e delle informazioni**. Tali attività, verranno dettagliate nelle sezioni successive (v. par. 5).

Nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, l'Amministrazione ha richiesto, ai fini dello sviluppo del **Progetto di Sicurezza,** l'esecuzione dei servizi afferenti al **Lotto 2 - Servizi di Compliance e controllo:**

- **Servizio di Security Strategy - L2.S16**
- **Vulnerability Assessment - L2.S17**
- **Supporto all'analisi e gestione degli incidenti - L2.S21**
- **Penetration Testing - L2.S22**
- **Compliance Normativa – L3.S23**

4.2 Servizi richiesti

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'**	**IMPORTO**
L2.S16	Security Strategy	L2.S16 - gg/p Team ottimale	2394	**598.500,00 €**
L2.S17	Vulnerability Assessment	L2.S17 - gg/p Team ottimale	242	**40.000,00 €**
L2.S21	Supporto all'analisi e gestione degli incidenti	L2.S21 - gg/p Team ottimale	147	**25.000,00 €**
L2.S22	Penetration Testing	L2.S22 - gg/p Team ottimale	508	**83.800,00 €**
L2.S23	Compliance normativa	L2.S23 - gg/p Team ottimale	353	**60.000,00 €**
			TOTALE	**807.300,00 €**

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

4.3.1.1. Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
PMO	Supporto al PMO/Technical Advisory per il coordinamento delle iniziative di sicurezza informatica anche con il sostegno di un team multidisciplinare esterno.	• *Attività di PMO*
Assessment della postura di sicurezza ed elaborazione di una roadmap evolutiva per le iniziative di sicurezza informatica	• Cyber Assessment trasversale volto all'attività di analisi di dettaglio delle procedure, processi, organizzazione ed alla consapevolezza delle capacità cyber e consolidamento del piano strategico delle iniziative tattiche; • Assessment verticale sulla gestione delle identità digitali e degli accessi logici, atto a definire l'attuale	• *Cyber Assessment (Executive summary)* • *Piano delle iniziative tattiche di sicurezza*

Macro-attività	Attività	Deliverable
	livello di maturità sulle modalità di gestione delle utenze; • Conduzione di attività di follow up dell'assessment con l'obiettivo di monitorare lo stato di evoluzione della postura a seguito degli interventi oggetto dell'intera progettualità; • Assessment verticali sull'operatività del personale presso i n.5 distretti provinciali; • Follow-up degli assessment verticali sull'operatività del personale presso i n.5 distretti provinciali.	• *Progetto di Sicurezza* • *Executive summary deep dive distretti provinciali (n. 5)*
Processi e corpo documentale	Definizione dei processi di sicurezza mediante la redazione del corpo documentale finalizzato alla definizione di ruoli e responsabilità interne ed esterne all'Ente. Nello specifico: • Revisione/redazione di n. 6 politiche di alto livello (es. Sicurezza delle Informazioni, Uso dei controlli crittografici, Politica di smartworking, Gestione dei Log, Hardening dei sistemi); • Revisione/redazione di n. 13 procedure operative di alto livello da redigere coerentemente con le politiche sviluppate (es. backup e restore; ciclo di vita delle identità; ricertificazione delle assegnazioni; monitoraggio degli accessi critici e privilegiati; security by design; processo di gestione delle vulnerabilità).	• *6 Politiche di Sicurezza di alto livello* • *13 Procedure operative di alto livello (coerentemente con le politiche*
Formazione	Potenziamento della consapevolezza del personale dell' Ente attraverso attività formative e informative come di seguito specificate. **a) Formazione rivolta ai Dirigenti:** Tale attività formativa prevede il supporto anche nella organizzazione/ingaggio/calendarizzazione delle sessioni e si sostanzia in: ○ Produzione del materiale di dettaglio in ambito Cybersecurity e Conformità Normativa ed erogazione di n. 2 edizioni, in aula fisica presso la sede dell'Ente, per i Dirigenti dell'Ente a copertura di tutta la popolazione in perimetro (per un totale di n.12h). Ogni edizione avrà n. 3 sessioni, ciascuna sessione avrà una durata di 2h e sarà basata sul medesimo contenuto in ambito Cybersecurity e Conformità Normativa; Per ogni modulo di formazione verrà effettuato un test di valutazione e la predisposizione di un report di sintesi che permetterà la predisposizione di reportistica consolidata per	• *Erogazione sessioni di formazione (come descritte nella colonna "Attività")* • *Newsletter mensile sulle best pratcice in materia di sicurezza informatica* • *Esecuzione di una esercitazione Table Top*

Macro-attività	Attività	Deliverable

valutare il livello di maturità cyber della Dirigenza e di informare ulteriori e successive iniziative di formazione.

In aggiunta, a valle delle sessioni formative sarà rilasciato un attestato di partecipazione unitamente ad un prontuario esplicativo relativo alle best practice di sicurezza in materia cyber e data protection;

b) Formazione rivolta al Personale IT/Security:

Tale attività formativa prevede il supporto anche nella organizzazione/ingaggio/calendarizzazione delle sessioni e si sostanzia in:

- Produzione del materiale ed erogazione di n. 4 sessioni formative (per un totale di n.12 h) sincrone al personale dell'Ente da erogare in aula fisica presso la sede dell'Ente. Ognuna delle sessioni avrà una durata di 3h il cui contenuto sarà selezionato, in base alle esigenze dell'ente ed in funzione alle categorie del Framework Nazionale della Cyber Security e Data Protection. I 4 moduli pertanto potranno essere erogati da personale tecnico su tematiche quali, a titolo meramente esemplificativo: Vulnerability Management, Gestione Terze Parti, Network security, Gestione delle Identità, ecc.

Per ogni sessione di formazione verrà effettuato un test di valutazione e la predisposizione di un report di sintesi che permetterà la predisposizione di reportistica consolidata per valutare il livello di maturità cyber del personale coinvolto e di informare ulteriori e successive iniziative di formazione;

c) Formazione rivolta al Personale amministrativo selezionato per coinvolgerli nelle attività di Business Impact Analysis:

Tale attività formativa prevede il supporto anche nella organizzazione/ingaggio/calendarizzazione delle sessioni e si sostanzia in:

- Produzione del materiale ed erogazione di n. 6 sessioni formative con medesimo contenuto (per un totale di n.12 h) sincrone al personale amministrativo, da erogare in aula fisica presso le sedi dell'Ente. Ognuna delle sessioni avrà una durata di 2h e sarà ripartita in n.2 moduli distinti:;
- 1,5h ora dedicata al contenuto in materia cybersecurity e sulle best practice di sicurezza da

Macro-attività	Attività	Deliverable

applicare nelle attività quotidiane e per introdurre le attività di Business Impact Analysis;

- 0.5h ora dedicata al contenuto in materia di conformità normativa

Per ogni modulo di formazione verrà effettuato un test di valutazione e la predisposizione di un report di sintesi che permetterà la predisposizione di reportistica consolidata per valutare il livello di maturità cyber della Dirigenza e di informare ulteriori e successive iniziative di formazione.

In aggiunta, a valle delle sessioni formative sarà rilasciato un attestato di partecipazione unitamente ad un prontuario esplicativo relativo alle best practice di sicurezza in materia cyber e data protection;

d) Formazione rivolta al Personale selezionato dei Dipartimenti:

Tale attività formativa prevede il supporto anche nella organizzazione/ ingaggio/ calendarizzazione delle sessioni e si sostanzia in:

- Produzione del materiale ed erogazione di n.13 sessioni formative ognuna delle quali avrà durata 2,5h con medesimo contenuto (per un totale di n.32,5 h) per il personale selezionato dei Dipartimenti erogate in aula fisica presso le sedi dei Dipartimenti.
- Nello specifico i workshop formativi avranno ad oggetto le principali best practice di sicurezza, la compliance normativa e le ulteriori tematiche in accordo con le esigenze dell'Ente.
- Produzione di una newsletter mensile sulle best pratice in materia di sicurezza informatica per le attività quotidiane da indirizzare a tutta la popolazione aziendale. Il servizio sarà mensile mediante la produzione di un'infografica e durerà per l'intera fornitura;

Per ogni sessione di formazione verrà effettuato un test di valutazione e la predisposizione di un report di sintesi che permetterà la predisposizione di reportistica consolidata per valutare il livello di maturità cyber del personale coinvolto e di informare ulteriori e successive iniziative di formazione;

In aggiunta, a valle delle sessioni formative sarà rilasciato un attestato di partecipazione unitamente ad un prontuario esplicativo relativo alle best practice di sicurezza in materia cyber e data protection;

Macro-attività	Attività	Deliverable
	e) Preparazione ed esecuzione di un Table top, nello specifico: Tale attività formativa prevede il supporto anche nella organizzazione/ingaggio/calendarizzazione delle sessioni e si sostanzia in: • Attività di formazione verticale di 1,5h in aula fisica dell'Ente in materia di gestione incidenti per il personale che compone le unità organizzative che possono essere incluse nell'ambito della gestione degli incidenti sulla base anche della procedura di incident management che sarà definita (es, Sistemi Informativi, Privacy/DPO, Direzione Generale, Comunicazione, Ufficio Gestione del Personale etc); • Organizzazione ed erogazione di una esercitazione Tabletop di ca. 3h, mirata a simulare scenari di incidente informatico, rivolta alle figure apicali dell'Ente (es, Direttori/ Dirigenti afferenti alle seguenti strutture: Sistemi Informativi, Privacy/DPO, Comunicazione, etc), al fine di preparare l'organizzazione a gestire tale tipologia di eventi e, quindi, ridurne l'impatto sulla normale operatività. L'attività consiste nell'identificazione degli scenari di crisi su cui effettuare le attività di testing e ha come obiettivo quello di sensibilizzare i partecipanti sul proprio ruolo nell'ambito della gestione degli incidenti di sicurezza, testare le capacità di risposta a potenziali situazioni di emergenza e crisi e comprendere gli impatti e le conseguenze che determinati scenari di crisi possono comportare; A valle dell'esercitazione verrà predisposto un report di sintesi che permetterà la predisposizione di reportistica per valutare pro, contro e ambiti di miglioramento delle modalità di risposta dell'Ente emerse durante l'esercitazione e di informare ulteriori e successive iniziative di formazione	
Analisi del rischio	• Definizione e adozione metodologia di analisi del rischio • Supporto operativo per l'esecuzione analisi dei rischi (Max 2 processi)	• *Metodologia di analisi del rischio* • *Executive summary risultati analisi del rischio*

Macro-attività	Attività	Deliverable
Continuità operativa	Definizione e formalizzazione del framework di Business Continuity Management in termini di scope, metodologie e modello organizzativo: • Definizione della metodologia di Business Impact Analysis • Esecuzione di Business Impact Analysis su un perimetro selezionato di processi/servizi critici su un massimo di 5 servizi/processi critici; • Recovery capabilities Assessment: valutazione degli impatti e definizione dei parametri RTO (Recovery Time Objective) e RPO (Recovery Point Objective) su massimo 5 servizi critici; • Definizione del modello di gestione della crisi ICT con identificazione di un workflow operativo di alto livello ed identificazione di ruoli e responsabilità; • Definizione strategie di continuità ICT e del piano di continuità operativa di alto livello	• *BIA* • *Crisis management* • *Recovery capabilities Assessment* • *Strategie di continuità ICT* • *Piano Cont. Operativa*
Gestione delle Terze Parti	• Redazione di Linee Guida per la definizione dei Requisiti di Sicurezza applicabili alle Terze Parti; • Analisi delle clausole contrattuali integrative dei contratti con le Terze Parti e feedback per opportuna declinazione in funzione del livello di rischio associato ai servizi erogati dal fornitore, per gli ambiti relativi alla sicurezza informatica; • Definizione di una metodologia di verifica dei fornitori; • Max 2 audit in modalità self-assessment sulla base del processo/metodologia definito ed eventuale verifica attraverso interviste da remoto delle risposte fornite dalle terze parti. • Follow-Up delle attività di audit su terze parti (max n.4 attività di follow up) e nuove n. 2 attività di audit da remoto a fornitori	• *Linee Guida* • *Clausole Contrattuali* • *Report Audit*

4.3.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO", si precisa che la modalità di remunerazione di tali servizi è di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La avverrà sulla base dello stato dell'avanzamento lavori mensile, determinato coerentemente con il piano di lavoro definito, e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.1.3 Attivazione e durata

Si prevede l'avvio del servizio a dicembre 2024 fino a dicembre 2025.

4.3.2 L2.S17 - Vulnerability assessment

4.3.2.1 Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Vulnerability Assessment	Attività di valutazione della robustezza dei controlli tecnici a presidio della sicurezza per un perimetro definito di sistemi infrastrutturali tradizionali ovvero IT, critici e non, riconducibili ad ARPAC, seguendo framework internazionali e standard di settore. Si richiede al RTI l'esecuzione di VA infrastrutturale max 2500 IP (2 run - fino a 1250 IP/run). L'attività di VA prevederà le seguenti fasi progettuali a titolo esemplificativo: o Identificazione del perimetro di sistemi, con rilevazione dei servizi e delle applicazioni critiche. o Definizione delle modalità operative di esecuzione delle analisi. o Esecuzione degli assessment, nello specifico considerando una serie di sistemi target che potranno comprendere applicazioni, host, sistemi, apparati, database, tutti identificabili mediante un IP address. Le tipologie di Vulnerability Assessment Interno richieste sono, a titolo esemplificativo e non esaustivo: • assessment sulle vulnerabilità nella rete (Network based vulnerability assessment • assessment sulle vulnerabilità nelle applicazioni individuate (Web Application Assessment)	• *VA Executive Summary* • *VA Technical Report* • *Remediation Plan*

Macro-attività	Attività	Deliverable
	• assessment sulle vulnerabilità nei computer: postazioni di lavoro definite sensibili (Host-based vulnerability assessment). o Analisi risultati e reportistica a livello executive e tecnica. o Definizione del piano di rimedio da attuare per eliminare le vulnerabilità riscontrate.	
Run *di Follow-Up (VA)*	Follow-up delle attività di VA infrastrutturale eseguita negli anni precedenti, 2500 IP (2 run - fino a 1250 IP/run). Tali attività verranno scelte e svolte secondo quanto descritto per l'attività principale.	• *VA Executive Summary* • *VA Technical Report* • *Remediation Plan*

4.3.2.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile, determinato coerentemente con il piano di lavoro definito, e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Penetration tester
- Junior Penetration tester

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.2.3 Attivazione e durata

Si prevede l'avvio del servizio a dicembre 2024 fino a dicembre 2025.

4.3.3 L2.S21 - Supporto all'analisi e gestione degli incidenti

4.3.3.1 Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Miglioramento del processo di Incident Management	Redazione del piano di risposta agli incidenti consistente in: • Procedura di Incident Management; • Template Incident response Report; • Incident response Playbooks (4 playbook).	• *Procedura di Incident Management* • *Template Incident response Report;*

4.3.3.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile, determinato coerentemente con il piano di lavoro definito, e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Security Analyst
- Junior Security Analyst
- Forensic Expert

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.3.3 Attivazione e durata

Si prevede l'avvio del servizio a dicembre 2024 fino a dicembre 2025.

4.3.4 L2.S22 – Penetration Testing

4.3.4.1. Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Penetration Test su Infrastrutture e Applicazioni	Attività di sfruttamento manuale delle vulnerabilità note afferenti a sistemi infrastrutturali tradizionali ovvero IT,	• *PT Executive Summary*

Macro-attività	Attività	Deliverable
	critici e non, riconducibili ad ARPAC, seguendo framework internazionali e standard di settore quali OWASP e OSSTMM. Le tecniche seguite mirano a coprire uno spettro di metodologie e di scenari quanto più possibile ampio e differenziato, al fine di individuare tutte le possibili tecniche di attacco e di intrusione a cui i target potrebbero essere soggetti. Verranno eseguite attività di WAPT Greybox (4 webapp target: 2 alta complessità, 1 media complessità, 1 bassa complessità). Ognuna di queste attività di PT prevederà le seguenti fasi progettuali: • Identificazione del perimetro di sistemi, con rilevazione dei servizi e delle applicazioni critiche. • Definizione delle modalità operative di esecuzione delle analisi (es.: black box, grey box, white box) e dei profili utente eventualmente da verificare (es: Profilo “guest”, Profilo “Admin”, ecc). • Esecuzione degli assessment, nello specifico considerando target sia applicativi che infrastrutturali, individuati in fase di definizione dei singoli sottoprogetti di PT. • Analisi risultati e reportistica a livello executive e tecnica. • Definizione del piano di rimedio da attuare per eliminare le vulnerabilità riscontrate. • La scelta delle applicazioni da sottoporre a PT sarà guidata dai seguenti fattori chiave: ○ Esistenza di portali esposti su Internet; ○ Distribuzione degli asset su Cloud oltre che on premises; ○ Tipologia di dati trattati (sensibili, sanitari, giudiziari, ecc); ○ Funzione di business esposta; ○ Complessità intrinseca dell’applicazione e suo livello di rischio cyber.	• *PT Technical Report* • *Remediation Plan*
Run *di Follow-Up (PT)*	Follow-up delle attività di Penetration Test su infrastrutture e applicazioni. Verranno eseguite attività di WAPT Greybox (4 webapp target: 2 alta complessità, 1 media complessità, 1 bassa complessità). Tali attività verranno scelte e svolte secondo quanto descritto per l’attività principale.	• *PT Executive Summary* • *PT Technical Report* • *Remediation Plan*

4.3.4.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.4.3 Attivazione e durata

Si prevede l'avvio del servizio a dicembre 2024 fino a dicembre 2025.

4.3.5 L2.S23 - Compliance normativa

4.3.5.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Governo della Conformità Privacy	Supporto operativo multidisciplinare alla U.O. Sistemi Informativi e Informatici, e relativi follow-up per l'esecuzione di attività volte alla compliance GDPR (es. aggiornamento del registro dei trattamenti con riferimento ai trattamenti di responsabilità della direzione sistemi informativi; revisione di processi e corpo documentale come (es. Procedura di Privacy by Design, Requisiti Privacy per lo Sviluppo, Template di Nomina AdS/Autorizzati, Procedura di Data Breach, Procedura di Gestione AdS, Procedura Gestione Richieste Interessati), Definizione di una Baseline misure di sicurezza; Focus se tematiche specifiche (es. Videosorveglianza), esecuzione di Data Protection Impact Assessment ecc.).	• *Supporto operativo multidisciplinare*

4.3.5.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Information Security Consultant
- Junior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.5.3 Attivazione e durata

Si prevede l'avvio del servizio a dicembre 2024 fino a dicembre 2025.

4.4 Indicatori di digitalizzazione

Nell'ambito delle attività di governance ed in particolare della valutazione del livello di efficacia degli interventi operati dalle Amministrazioni attraverso l'utilizzo di contratti esecutivi afferenti alle Gare Strategiche in ambito Sicurezza ICT, si intendono definite due tipologie di indicatori:

- **Indicatori Generali**, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale;
- **Indicatori Specifici**, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti. In tale contesto, è definito un indicatore (cd. "indicatore di progresso" in seguito descritto) che indica il livello di maturità della infrastruttura di sicurezza ICT delle Amministrazioni, sulla base del grado di mappatura degli interventi effettuati con le misure minime di sicurezza AGID (Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»).

Gli indicatori saranno utilizzati per il monitoraggio dei contratti e del raggiungimento dei relativi obiettivi.

Nel contesto di ARPAC, per la tipologia di interventi previsti, si considerano gli indicatori presentati nei prossimi due paragrafi e che saranno oggetto di monitoraggio nell'intero arco temporale dell'incarico presentato in questo Piano Operativo.

4.4.1 Indicatori generali di digitalizzazione

Di seguito si riportano gli indicatori Generali di digitalizzazione previsti per la presente fornitura:

	INDICATORI DI COLLABORAZIONE E RIUSO	VALORE EX ANTE	VALORE EX POST
1	**Obiettivi CAD raggiunti con l'intervento**	*Dato da valorizzare all'inizio dell'incarico*	*Dato da valorizzare ogni 12 mesi*

Per l'indicatore riportato sopra, verrà effettuata una valutazione in fase di avvio degli interventi progettuali e a valle (ogni 12 mesi), così da misurare il livello di digitalizzazione raggiunto.

4.4.2 Indicatori di progresso

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

Lo studio della effettiva applicabilità e la conseguente scelta e valorizzazione ex-ante ed ex-post degli indicatori di progresso è una delle attività previste in questo Piano Operativo all'interno dei servizi di "Cyber Maturity Assessment" previsto all'interno della gamma di servizi L2.S16 – Security Strategy.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività saranno svolte dalle aziende secondo la ripartizione seguente:

SERVIZIO	Deloitte Risk Advisory	EY Advisory	Teleco
L2.S16	79,62%	20,38%	0,00%
L2.S17	0,00%	100,00%	0,00%
L2.S21	100,00%	0,00%	0,00%
L2.S22	0,00%	100,00%	0,00%
L2.S23	100,00%	0,00%	0,00%
TOTALE	69,55%	30,45%	0,00%

5.2 Modalità di ricorso al subappalto da parte del fornitore

SERVIZIO	AZIENDA RTI	QUOTA SUBAPPALTABILE	SUBAPPALTATORE
L2.S16, L2.S17,, L2.S21, L2.S22, L2.S23	**DLT R.A.- EY-TELECO**	**50%**	**DA DEFINIRE**

Si precisa che la quota di subappalto della singola Società non potrà mai essere superiore alla quota massima subappaltabile fatta salva espressa deroga concessa dal Committente.

5.3 Organizzazione e figure di riferimento del fornitore

In relazione all'organizzazione e alle figure di riferimento del Fornitore per la conduzione del progetto, si prevede la presenza di un RUAC con una struttura di Governance a supporto per le attività di PMO. In particolare, il **RUAC del CE** collabora con il RUAC di AQ ed è responsabile dei servizi del singolo CE.

Per l'erogazione dei servizi è prevista la presenza del referente tecnico per ciascun CE e comunque per ciascuna Amministrazione per tutti i servizi del Lotto 2 - Referente Tecnico CE (RT) - che assicura il corretto svolgimento dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori condivisi. Per ciascun servizio oggetto del presente Piano Operativo, l'organizzazione prevede la composizione di un gruppo dedicato composto da un **Responsabile Attività** e da un gruppo di lavoro di supporto.

RUOLO	NOMINATIVI
RUAC CE	Fabio Battelli
Referente Tecnico CE (RT)	Marco Ceccon
Responsabile Attività L2.S16	Biagio Salerno
Responsabile Attività L2.S17	Rodolfo Mecozzi
Responsabile Attività L2.S21	Biagio Salerno
Responsabile Attività L2.S22	Rodolfo Mecozzi
Responsabile Attività L2.S23	Biagio Salerno

5.4 Modalità di esecuzione dei servizi

Le attività relative all'esecuzione dei servizi saranno svolte presso gli uffici del Fornitore e, ove necessario e/o richiesto per l'espletamento delle attività contrattuali, presso l'Amministrazione richiedente.

6 Piano di lavoro

6.1 Piano di Presa in carico

Il piano di presa in carico si basa sul coinvolgimento del personale che verrà poi impegnato a regime nella fornitura, sia a livello di governo che di erogazione dei servizi e trasparenza sull'andamento del processo di subentro nei confronti di tutti gli attori interessati attraverso una governance operativa e focalizzata.

FASE	ATTIVITÀ	W1	W2	W3	W4	W5
Pianificazione	Pianificazione delle attività					
Predisposizione Strumenti	Predisposizione e aggiornamento strumenti					
Assessment documentale	Analisi AS IS dei progetti in corso					
Acquisizione competenze	Incontri con il personale dell'Amministrazione e del fornitore uscente, training on the job, self training, workshop					
Ottimizzazione	Individuazione delle possibili aree di miglioramento					
Fine presa in carico	Ricognizione e verifica delle attività svolte					
Governance	Verifica dello stato delle attività					

6.2 Cronoprogramma, copia pianificazione

Di seguito si riporta la pianificazione di massima dei servizi previsti:

	Mese 1	Mese 2	Mese 3	Mese 4	Mese 5	Mese 6	Mese 7	Mese 8	Mese 9	Mese 10	Mese 11	Mese 12	Mese 13
L2.S16													
L2.S17													
L2.S21													
L2.S22													
L2.S23													

Le milestone e i deliverable specifici relativi a ciascuna delle attività verranno preventivamente concordate con l'amministrazione.

6.3 Data di attivazione e durata del servizio

Il contratto esecutivo avrà i suoi effetti dalla data di stipula e avrà una durata complessiva di 13 mesi dalla data di attivazione dei servizi, compatibilmente con il vincolo definito dall'Accordo quadro, ovvero che i Contratti Esecutivi abbiano una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

7 Piano della qualità specifico

7.1 Organizzazione dei Servizi

A Livello di gestione del contratto esecutivo sono state identificate le seguenti figure con le relative responsabilità:

- **Responsabili dei Servizi (RdS):** per ciascun servizio è individuato un responsabile che supporta i Referenti Tecnici dei CE assicurando omogeneità di approccio trasversalmente alle diverse Amministrazioni e abilitando il riuso delle soluzioni già applicate con successo su altri CE.
- **RUAC CE:** figura responsabile dell'attuazione del CE, rappresenta il RTI nei confronti della singola Amministrazione.
- **Referente Tecnico CE (RT)** per l'erogazione dei servizi, assicura il corretto svolgimento dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori condivisi. Ha la responsabilità delle attività di Presa in carico e trasferimento di Know How durante le quali è il riferimento per il fornitore uscente/entrante e coordina le attività dei team di lavoro.
- **Responsabile Attività** è referente tecnico per ciascuna attività all'interno del CE, coordina e assicura il corretto svolgimento delle attività operative eseguite dal team di lavoro.
- **Team di Lavoro (TL),** team operativi di intervento impegnati nell'erogazione dei servizi, composti da professionisti con profili previsti.

Nei successivi paragrafi sono declinate le figure previste all'interno del Team di Lavoro di ciascun servizio.

Security Strategy (L2.S16)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Security Solution Architect	Figura professionale dedicata al mantenimento della sicurezza del sistema informatico di un'organizzazione. Sarà responsabile dell'analisi dell'infrastruttura IT e delle relazioni tra i differenti sistemi e componenti infrastrutturali volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza. Si occuperà, inoltre, dell'analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza).
Senior Information Security Consultant	Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per

	tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
Senior Security Auditor	Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Completa i giornali di audit documentando test e risultati dell'audit. Individua i possibili punti vulnerabili di un sistema informativo.
Data Protection Specialist	Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche, verifica il rispetto di quanto previsto nelle normative italiane ed europee in termini di protezione dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali.

Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

Vulnerability Assessment (L2.S17)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.

Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

Supporto all'analisi e gestione degli incidenti (L2.S21)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal

	concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia Responsabile del coordinamento delle figure più Junior.
Junior Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

Penetration Testing (L2.S22)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

Compliance normativa (L2.S23)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Information Security Consultant	Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
Junior Information Security Consultant	Contribuisce nell'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) partecipando al ruolo di raccordo tra la struttura di governance della Cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni.
Senior Security Auditor	Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Completa i giornali di audit documentando test e risultati dell'audit. Individua i possibili punti vulnerabili di un sistema informativo.
Data Protection Specialist	Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche, verifica il rispetto di quanto previsto nelle normative italiane ed europee in termini di protezione dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali

Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

7.2 Metodologie e Tecniche

Security Strategy (L2.S16)

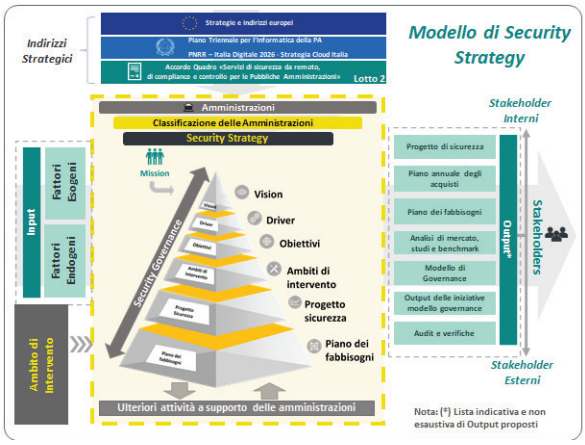
La strategia di sicurezza è l'abilitatore fondamentale che consente di individuare le azioni più appropriate per gestire i rischi di sicurezza in coerenza con le specificità delle Amministrazioni individuando le modalità con

cui raggiungere i livelli di sicurezza richiesti e al contempo assicurare la conformità alle normative vigenti ed alle direttive di settore.

L'approccio concreto di elaborazione del Progetto di Sicurezza (di seguito PdS) avviene tramite modelli di PdS differenziati sulla base della classificazione e della complessità delle Amministrazioni (MappaPA).

Allo scopo di supportare le Amministrazioni nella pianificazione strategica della Sicurezza ICT, il RTI prevede l'utilizzo di uno specifico Modello di Security Strategy, sviluppato sulla base di standard e leading practices riconosciute in ambito Security ICT (es. ISO27001-2, ISO27017-8, ISO27701 ISO31000, ISA62443, NIST800.53 v5, Framework Nazionale, Linee guida ENISA).

Tramite tale modello l'Amministrazione sarà in grado di recepire gli indirizzi strategici (a livello nazionale ed europeo) e gli input esogeni ed endogeni, per definire - attraverso l'ausilio di metodologie, approcci operativi e strumenti - il PdS. Il PdS, coerentemente con il contesto di riferimento e con le esigenze di stakeholder interni ed esterni, avrà lo scopo di attuare la Missione e la derivata Visione dell'Amministrazione (i.e. la trasposizione della Missione in una strategia a lungo termine di evoluzione tecnologica e/o organizzativa mirata al suo soddisfacimento). Con riferimento agli ambiti del PdS, allo scopo di articolare una risposta completa rispetto a tutte le fasi del ciclo di vita della sicurezza delle informazioni e dei sistemi ICT, il RTI propone di considerare, a titolo indicativo e non esaustivo, i seguenti Ambiti di intervento:



- Identify: strategia e pianificazione, Governance Asset e Processi, gestione del rischio cyber, security assurance (VA, PT, Testing del Codice), sicurezza terze parti e contratti di servizio, Compliance normativa;
- Protect (Management): Information & Data Security, Identity & Access Management, Security by Design e Secure SDLC, Application & System Protection, Network Protection, Data Center Security, Secure Cloud Computing, Cyber Awareness & Training, Security Operations;
- Detect: Monitoraggio continuo di sicurezza, Incident Detection, Threat intelligence, Threat Hunting;
- Response: Cyber Incident Response, Investigation and Forensics
- Recovery: Continuità Operativa and Crisis Management, Disaster Recovery.

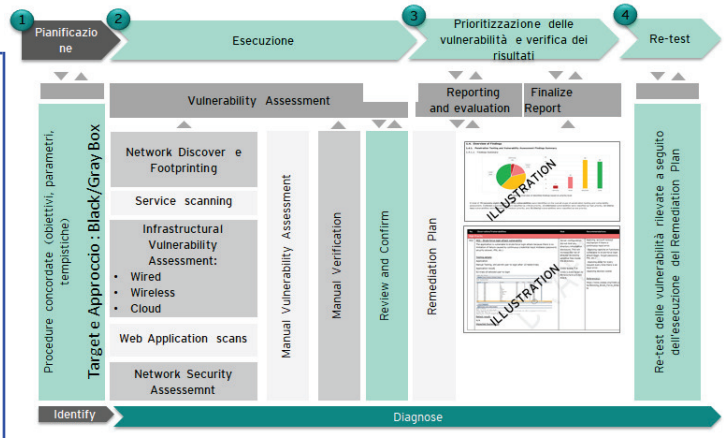
Vulnerability Assessment (L2.S17)

Il servizio di Vulnerability Assessment prevede l'identificazione in maniera proattiva, mediante una verifica dinamica della sicurezza, delle vulnerabilità presenti su dispositivi di rete, software e applicazioni delle Amministrazioni e la mitigazione dei rischi cyber connessi. Il RTI eroga le attività in ambito al presente servizio facendo affidamento sugli elementi distintivi sotto riportati.

1. Standardizzazione del reporting e dei piani di prioritizzazione/remediation attraverso l'utilizzo di una piattaforma centralizzata (denominata Bug Blast) ed indipendente dai motori di scansione (vulnerability scanner), garantendo ripetibilità ed uniformità dei risultati;
2. Metodologia per la definizione dei "remediation plan" con approccio risk-based e reportistica in grado di rappresentare le vulnerabilità identificate sia ad interlocutori executive che tecnici, fornendo pratici strumenti operativi per agevolare la risoluzione delle stesse;

3. Centri di eccellenza nazionali ed internazionali in ambito Cybersecurity (Roma, Milano, Bari, ed oltre 10 in EU), con la presenza di laboratori specialistici e con professionalità verticali su attività di Offensive Security. Tali centri supportano i team nella raccolta di informazioni relative a nuove vulnerabilità (es. mediante tecniche di Cyber Threat Intelligence) e tecniche innovative per lo sfruttamento delle stesse;
4. Eterogeneità nella copertura degli ambienti target (IT/OT/IoT/Cloud) attraverso strumenti e tecniche idonee e specifiche a garantire il discovery per ciascuna tipologia di target;
5. Ampio supporto nel discovery di misconfiguration e vulnerability specifiche per gli ambienti di cloud computing (IaaS, PaaS, SaaS), anche in presenza di CSP differenti (AWS, Azure, Google, ecc.).

Le attività di Vulnerability Assessment (VA) forniranno evidenze di dettaglio sulle vulnerabilità riconducibili all'infrastruttura ICT e IoT/OT, funzionali anche ad elaborare una baseline iniziale del livello di vulnerabilità e di esposizione del sistema informativo dell'Amministrazione. L'attività sarà svolta sia con strumenti automatici sia con strumenti definiti ad-hoc sulla base della tipologia del target oggetto di analisi. Il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei VA. Le attività di VA eseguite sono basate sulle metodologie OSSTMM, OWASP, PTES, NIST 800-52/53 e ISA 62443, riconosciute globalmente come standard de-facto.



L'applicazione di tali metodologie garantirà risultati coerenti, ripetibili e misurabili. Nell'ambito delle attività di VA terremo in considerazione il sempre più diffuso utilizzo delle tecnologie Cloud da parte delle Amministrazione, in coerenza con quanto definito dalla Strategia Cloud Italia. A tal fine, su specifica richiesta dell'Amministrazione, il RTI è in grado di integrare all'interno dei servizi offerti anche l'esecuzione di attività di Assessment del livello di sicurezza dei servizi Cloud IaaS e SaaS, verificandone la compliance rispetto a standard, requisiti normativi e best practice di settore, e ricercando vulnerabilità celate negli errori di configurazione dei diversi ambienti cloud. Il RTI potrà eseguire le attività di VA in maniera periodica ove richiesto e ritenuto opportuno.
Per l'esecuzione dei servizi richiesti dall'Amministrazione, la metodologia prevede l'esecuzione di 4 fasi progettuali:

- Pianificazione delle attività,
- Esecuzione dei Vulnerability Assessment,
- Proritizzazione delle vulnerabilità e verifica dei risultati,
- Re-test delle vulnerabilità a seguito del remediation plan.

Il RTI propone l'adozione di una piattaforma specifica per l'esecuzione di attività di Vulnerability Assessment. La Piattaforma Bug Blast ha l'obiettivo di fornire report personalizzati e di tracciare le vulnerabilità dalla fase di discovery e per tutte le fasi di remediation. Le informazioni che afferiscono alle attività di VA richieste saranno disponibili nel portale tramite un sistema di autorizzazione granulare e le Amministrazioni potrà accedere a tali informazioni sulla base del periodo di retention che sarà concordato di volta in volta con le stesse e comunque, salvo diversa indicazione da parte dell'Amministrazione e nel rispetto delle normative vigenti, per un periodo garantito non inferiore a 1 mese dalla fine delle attività. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con le stesse. Approccio operativo. L'approccio operativo

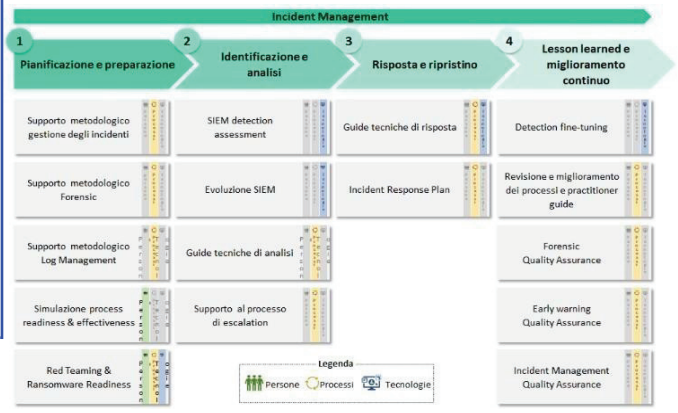
proposto dal RTI prevede l'esecuzione di tutte le attività tecniche previste dal CTS. I relativi risultati saranno analizzati e correlati dal Team operativo. Ove possibile, per le vulnerabilità rilevate sarà effettuata una verifica manuale al fine di identificare ed eliminare i falsi positivi; tale attività è svolta mediante processi innovativi di controllo, sviluppati nel corso delle esperienze in ambito Offensive Security e tramite il supporto dei Centri di eccellenza del RTI, che consentono di ridurre al minimo la presenza di errori.

Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio:

Ambito di utilizzo	Principali strumenti
Vulnerability Assessment	● **Open Source**: Kali Linux, nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan, Shodan, Zoomeye, Censys, Air-Ng tools, Wifite, Airgeddon, Wireshark. ● **Di Mercato**: Nessus, Hak5 WiFi, Burp Proxy Professional. ● **Proprietario**: Bug Blast
Cloud Security Assessment	● **Di Mercato**: Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM)
Vulnerability Assessment IoT	● **Open Source**: Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, HackRF (HW), ZigDiggity, Proxmark (HW), TLSAssistant. ● **Di Mercato**: Burp Proxy Professional

Supporto all'analisi e gestione degli incidenti (L2.S21)

Il servizio di supporto all'analisi e gestione degli incidenti prevede lo svolgimento da parte del RTI di attività consulenziali volte a incrementare efficacia ed efficienza dei processi di Forensic e Incident Management, nelle fasi di analisi, progettazione e verifica (post-mortem) di tali processi, nonché di supporto alla divulgazione delle informazioni. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi elencati di seguito:



1. Coinvolgimento di risorse con ampia e riconosciuta esperienza nella realizzazione di CERT e SOC in Italia e nel mondo per organizzazioni pubbliche e private di primaria importanza. Il RTI ha inoltre supportato 7 delle 11 organizzazioni italiane che hanno accreditato i loro CERT alla community internazionale FIRST
2. Coinvolgimento di risorse che hanno contribuito direttamente allo sviluppo delle pratiche di Incident Readiness come dimostrato dalla pubblicazione di numerosi studi nazionali e internazionali.
3. Disponibilità di una libreria proprietaria composta da oltre 350 Use Case di monitoraggio costantemente aggiornata sulla base delle esperienze acquisite presso i clienti del network a livello globale, evoluzioni tecnologiche, trasformazioni nelle tattiche, tecniche e procedure (TTP) utilizzate dagli attori di minaccia in diverse tipologie di ambienti (es. cloud SaaS, PaaS e IaaS, Mobile, IoT, ecc.)
4. Disponibilità di framework proprietari, sviluppati internamente dal RTI e aggiornati in maniera continuativa sulla base delle esperienze acquisite e di report specialistici di settore, per la valutazione del livello di maturità

di CERT e SOC e l'identificazione delle tecnologie di sicurezza a supporto delle attività di gestione degli incidenti
5. Team di lavoro multidisciplinare altamente qualificato e certificato in ambito Forensic, Security Defense e Offense.

Il servizio di supporto all'analisi e gestione degli incidenti proposto affronta la tematica in modo olistico e multidisciplinare. Al fine di raggiungere tali obiettivi, il RTI supporta l'Amministrazione al fine di abilitare il corretto svolgimento di ciascuna delle fasi di gestione degli incidenti attraverso attività consulenziali da svolgersi in maniera preventiva come supporto all'intero processo (analisi e progettazione) e definire un processo strutturato di Forensic e verificarne l'efficacia (verifica).

A) Incident Management

Il RTI propone un approccio strutturato al supporto in ambito gestione incidenti, che prevede l'esecuzione di attività di natura consulenziale da svolgersi preventivamente per guidare il corretto svolgimento del servizio di Incident Management da parte dell'Amministrazione. Ciascuna delle attività proposte consentirà di abilitare lo svolgimento e incrementare l'efficacia di una diversa fase del processo di Incident Management, come di seguito riportato:

- A.1 Pianificazione e preparazione: una fase di preparazione correttamente eseguita e personalizzata sulla base del contesto permette di minimizzare gli impatti degli incidenti, facendo leva su un'adeguata infrastruttura tecnologica di sicurezza e personale specializzato.
- A.2 Identificazione e analisi: la fase di identificazione e analisi di un incidente ha l'obiettivo di monitorare in modo centralizzato gli eventi di sicurezza provenienti da fonti strutturate (es. SIEM) e non strutturate (es. e-mail da utenti) per rilevare minacce miranti agli asset e ai servizi della PA, analizzarli per comprendere se si tratti di un falso positivo che necessita di azioni correttive o di un incidente con potenziale impatto sul perimetro e classificare e prioritizzarne la gestione sulla base di criteri definiti.
- A.3 Risposta e ripristino: tale fase prevede l'identificazione e l'implementazione delle azioni di contenimento a breve termine dell'incidente, con l'obiettivo di limitare le conseguenze dell'incidente e ripristinare la normale operatività in maniera tempestiva ed efficace.
- A.4 Lesson learned e miglioramento continuo: tale fase prevede, immediatamente a valle della gestione di un incidente, una valutazione ex-post della stessa per verificare che le attività siano state condotte in conformità con quanto previsto dal processo, e un'attività periodica volta a identificare eventuali punti di miglioramento nelle attività svolte attraverso l'elaborazione di reportistica, lo svolgimento di meeting ricorrenti per condividere eventuali gap e relative azioni di rimedio.

B) Forensic

Le attività di supporto all'Amministrazione nella gestione di incidenti di sicurezza prevedono un approccio sinergico, finalizzato a incrementare l'efficienza delle modalità di intervento e dei tempi di reazione da parte dell'Amministrazione, in particolare nell'analisi forense post-mortem degli incidenti.
Le attività di supporto erogate nei confronti dell'Amministrazione prevedranno una costante verifica di quality assurance da parte di profili esperti, al fine di garantire un elevato livello qualitativo dell'esecuzione del processo di Forensic.

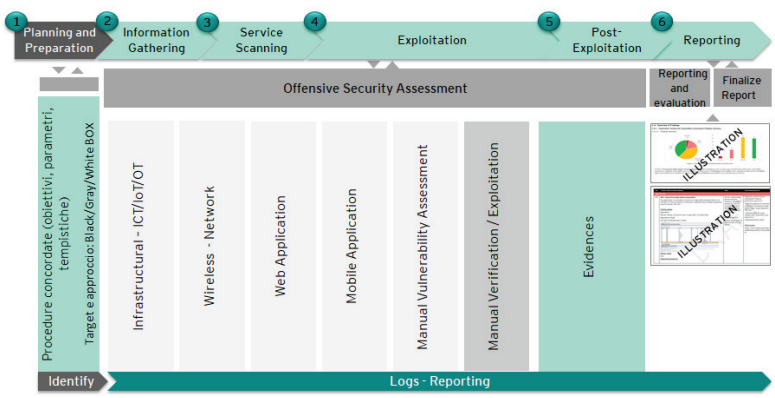
- Definizione di un template di catena di custodia per supportare i team di Forensic nel tracciamento delle attività eseguite sulle evidenze acquisite;

- Definizione di un processo di Forensic secondo best practice volto a definire ruoli, responsabilità, principi e attività operative che regolano il processo stesso;
- Governo (organizzazione, pianificazione, coordinamento, controllo) delle attività di verifica tecnica (quality assurance) del processo di Forensic.

Penetration Testing (L2.S22)

Il servizio di Penetration Test prevede l'esecuzione di attacchi simulati per verificare concretamente la possibilità di sfruttare vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi delle Amministrazioni. L'approccio offensivo consente di ottenere una chiara percezione degli effettivi livelli di esposizione/compromissione dei target analizzati, determinando la capacità di difesa e resilienza rispetto agli attacchi Cyber e fornendo conseguentemente elementi concreti per adeguare le misure di contrasto e protezione. Il servizio proposto è fondato sugli elementi distintivi sotto riportati:

1. Eccellenza del team di Ethical Hacking dimostrata dalla pubblicazione regolare di Common Vulnerabilities and Exposures (CVE) elenco di vulnerabilità divulgate pubblicamente e Zero Day, condivise attraverso i metodi di "Responsible Disclosure";
2. Copertura completa dei principali vettori di attacco per ogni singola sessione e tipologia di target, acquisita mediante l'aggiornamento continuo di un archivio centralizzato contenente il Threat Modelling e relative Tactics, Techniques and Procedures (TTP), alimentato dal team di Pen Tester coinvolti a livello globale nell'erogazione di tali servizi;



3. Utilizzo estensivo di fonti Cyber Threat Intelligence (OSINT e CLOSINT) con copertura geografica mondiale, derivante dai servizi di sicurezza gestista (SOC) del RTI, che consentono al Pen Tester di ottenere un quadro più ampio dell'effettivo livello di esposizione dei target in analisi, come ad esempio compromissioni/vulnerabilità/tecniche pubblicate nel dark web o in community specifiche, potenzialmente accessibili anche agli attaccanti e sfruttabili per realizzare una reale compromissione,;
4. Molteplicità di laboratori a livello nazionale ed internazionale con personale, strumenti ed infrastrutture dedicate alle attività di offensive security, con possibilità di verificare costantemente i vettori e le tecniche di attacco in ambienti simulati e su dispositivi di test; tali laboratori sono impiegati anche per addestramento, formazione ed aggiornamento continuo dei Pen Tester.

Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio.

Ambito di utilizzo	Principali strumenti
PT Infrastrutturale	● **Open Source**: nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan,scapy,hping, CrackMapExec, Air-Ng tools, Wifite, Airgeddon, Wireshark; ● **Di Mercato:** Acrylic WIFI **,** Hak5 Wifi (HW e SW), Nessus
PT Applicativo	● **Open Source**: Objection, Frida ,Apktool, Dex2jar, Hopper, Drozer, MobSF, Clang Static Analyzer,

Ambito di utilizzo	Principali strumenti
	Andrubis, Flawfinder, ApkAnalyser, Androwarn, Ghidra, Radare; ● **Di Mercato:** Nessus, Burp Proxy Professional
PT Device IOT	● **Open Source**: Burp Proxy Professional, Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, ZigDiggity; ● **Di Mercato:** HackRF, Proxmark
Red Team	● **Open Source**: Social Engineering Toolkit (SET) , Gophish , Invoke-Obfuscation, Veil Framework, Empire Project, DNSExfiltrator, Cloakify Factory; ● **Di Mercato:** Cobalt Strike, Metasploit Pro

Compliance normativa (L2.S23)

Il servizio di Compliance normativa prevede la definizione di un Sistema di gestione della Privacy in grado di governare in un'ottica di lungo periodo tutti gli adempimenti GDPR impattanti sui sistemi IT. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi elencati di seguito:

- Multidisciplinarietà delle competenze (IT, legali, operative e organizzative) integrate in team strutturati.
- Utilizzo del GDPR Compliance Framework (GDPR CF), che include la metodologia per lo svolgimento delle attività, modelli, processi, questionari, baseline di requisiti, strumenti automatizzati, in grado efficientare le attività progettuali
- Costante aggiornamento normativo realizzato attraverso l'Osservatorio Privacy del RTI
- DRA ed EYA si possono avvalere della collaborazione dei propri Studi Legali Associati.

Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un fattore abilitante per il trattamento dei dati da parte dell'Amministrazione e garantire agli interessati la protezione dei dati personali. A tale scopo, il RTI utilizzerà, per guidare lo svolgimento delle attività, il GDPR Compliance Framework (GDPR CF). Tale strumento propone una metodologia per la definizione e mantenimento del sistema privacy ed è caratterizzato da un ciclo di 4 fasi: a) Analisi; b) Implementazione; c) Verifica; d) Continuous Improvement. Quest'ultima fase è abilitata dal Privacy Maturity Model (PMM), ovvero uno strumento in grado di intercettare nel continuo, i punti di forza e di miglioramento del Sistema di gestione della privacy esprimendo lo stato di maturità e identificando in modo dinamico le aree di intervento. L'utilizzo del GDPR CF, oltre a mettere a disposizione un set esaustivo di strumenti automatici, potrà, essere supportato da un prodotto software integrato che consente di gestire il Sistema Privacy in modalità condivisa e collaborativa tra tutti i soggetti interessati (es. DPO, Privacy Officer, IT, Sicurezza, Risorse Umane, Acquisti).

Analisi: la fase di analisi prevede lo svolgimento di un assessment per verificare lo stato di conformità alla normativa applicabile da parte delle Amministrazioni al fine di comprendere le aree maggiormente a rischio e identificare gli eventuali interventi di rimedio necessari per garantire conformità e allo stesso tempo automatizzare i processi privacy.

Implementazione. tale fase consentirà di indirizzare le azioni di rimedio emerse a seguito dell'Assessment ed incluse nel Piano degli interventi o già previste dai piani di conformità dell'Amministrazione. Allo scopo di massimizzare l'efficacia degli interventi e la logica del riuso, le attività di implementazione sono eseguite secondo un modello operativo che prevede la messa a disposizione di template consolidati per le componenti del framework documentale (es. politiche, procedure, metodologie, nomine a responsabile, informative,

data processing agreement, materiale formativo) che saranno condivisi con l'Amministrazione e personalizzati sulla base delle specifiche necessità

Verifica: tale fase consente di misurare l'effettiva implementazione dei requisiti normativi a cui è soggetta l'Amministrazione, valutare il rischio derivante dai gap ed il livello di maturità raggiunto, proponendo eventuali punti di miglioramento, attraverso piani di azione costantemente monitorati.

Continuous Improvement: al fine di trasformare la privacy da adempimento di legge ad abilitatore "mandatorio" e cogliere tempestivamente i rischi normativi/sanzionatori/IT, si prevede l'adozione del PMM (o in alternativa il Data Protection Maturity Self-Assessment Model rilasciato dal CNIL).

consip

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO F

ID 2296

SCHEMA DI CONTRATTO ESECUTIVO – LOTTO 2

INDICE

CONTRATTO ESECUTIVO

TRA

_____, con sede in _____, Via _____, C.F. _____, nella persona nella persona di _____, in qualità di _____, giusta i poteri conferitigli da _____in data _____ (nel seguito per brevità anche "***Amministrazione***"),

E

_____, sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, Via ___, in persona del ___ e legale rappresentante Dott. ___, giusta poteri allo stesso conferiti da ___ (nel seguito per brevità anche "Fornitore");

OPPURE

- _____, sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, Via ___, in persona del ___ e legale rappresentante Dott. ___, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa la mandante _____ ___ con sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, via ___, e la mandante ___, con sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, via ___, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in _____ dott. _____ repertorio n. _____;

(nel seguito per brevità congiuntamente anche "Fornitore" o "Impresa")

PREMESSO CHE

(A) l'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, ha stabilito che Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311";

(B) L'articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip S.p.A. di concludere Accordi Quadro a cui le Stazioni Appaltanti, possono fare ricorso per l'acquisto di beni e di servizi.

(C) Peraltro, l'utilizzazione dello strumento dell'Accordo Quadro e, quindi, una gestione in forma associata della procedura di scelta del contraente, mediante aggregazione della domanda di più soggetti, consente la razionalizzazione della spesa di beni e servizi, il supporto alla programmazione dei fabbisogni, la semplificazione e standardizzazione delle procedure di acquisto, il conseguimento di economie di scala, una maggiore trasparenza delle procedure di gara, il miglioramento della responsabilizzazione e del controllo della spesa, un incremento della specializzazione delle competenze, una maggiore efficienza nell'interazione fra Amministrazione e mercato e, non ultimo, un risparmio nelle spese di gestione della procedura medesima.

(D) In particolare, in forza di quanto stabilito dall'art. 1, comma 514, della legge 28 dicembre 2015, n.208 (Legge di stabilità 2016) ,"Ai fini di cui al comma 512," – e quindi per rispondere alle esigenze delle amministrazioni pubbliche e delle società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 19 – "Consip S.p.A. o il soggetto aggregatore interessato sentita l'Agid per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. […] Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni".

(E) L'art. 20, comma 4, del D.L. n. 83/2012, come convertito con modificazioni dalla Legge 7 agosto 2012, n. 134, ha affidato a Consip S.p.A., a decorrere dalla data di entrata in vigore della legge di conversione del decreto medesimo, "le attività amministrative, contrattuali e strumentali già attribuite a DigitPA, ai fini della realizzazione e gestione dei progetti in materia, nel rispetto delle disposizioni del comma 3".

(F) Ai fini del perseguimento degli obiettivi di cui al citato Piano triennale per l'informatica nella Pubblica Amministrazione, e che in esecuzione di quanto precede, Consip S.p.A., in qualità di stazione appaltante e centrale di committenza, ha indetto con Bando di gara pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. ____ del _____ e nella Gazzetta Ufficiale dell'Unione Europea n. _____ del _____, una procedura aperta per la stipula di un Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, ai sensi dell'art. 54, comma 4, lett. a) del D. Lgs. n. 50/2016, con più operatori.

(G) Il Fornitore è risultato aggiudicatario della quota PAL del Lotto 2 della predetta gara, ed ha stipulato il relativo Accordo Quadro in data _____.

(H) In applicazione di quanto stabilito nel predetto Accordo Quadro, ciascuna Amministrazione Contraente utilizza il medesimo per la stipula di Contratti esecutivi, secondo quanto disciplinato nell'Accordo Quadro stesso.

(I) L'Amministrazione Contraente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto esecutivo, in conformità alle previsioni di cui al Capitolato Tecnico Generale.

(J) Il Fornitore dichiara che quanto risulta dall'Accordo Quadro e dai suoi allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico (Generale e Speciale) dell'Accordo Quadro, nonché dal presente Contratto esecutivo e dai suoi allegati, definisce in modo adeguato e completo gli impegni assunti con la firma del presente Contratto, nonché l'oggetto dei prodotti e dei servizi connessi da fornire e, in ogni caso, che ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica degli stessi e per la formulazione dell'offerta che ritiene pienamente remunerativa;

(K) il CIG del presente Contratto Esecutivo è il seguente: _____;

(L) <*ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3*> il CUP (Codice Unico Progetto) del presente Contratto Esecutivo è il seguente: _____;

TUTTO CIÒ PREMESSO SI CONVIENE E SI STIPULA QUANTO SEGUE:

1. DEFINIZIONI

1.1 I termini contenuti nel presente Contratto esecutivo hanno il significato specificato nell'Accordo Quadro e nei relativi Allegati, salvo che il contesto delle singole clausole disponga diversamente.

1.2 I termini tecnici contenuti nel presente Contratto esecutivo hanno il significato specificato nel Capitolato Tecnico Generale e Speciale, salvo che il contesto delle singole clausole disponga diversamente.

1.3 Il presente Contratto esecutivo è regolato:

a) dalle disposizioni del presente atto e dai suoi allegati, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti tra il Fornitore e l'Amministrazione relativamente alle attività e prestazioni contrattuali;
b) dalle disposizioni dell'Accordo Quadro e dai suoi allegati;
c) dalle disposizioni del D.Lgs. 50/2016 e s.m.i. e relative prassi e disposizioni attuative;
d) dalle disposizioni di cui al D.Lgs. n. 82/2005;
e) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato.

2. VALORE DELLE PREMESSE E DEGLI ALLEGATI

2.1 Le premesse di cui sopra, gli atti e i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Contratto esecutivo.

2.2 Costituiscono, altresì, parte integrante e sostanziale del presente Contratto esecutivo:

- l'Accordo Quadro,
- gli Allegati dell'Accordo Quadro,
- l'**Allegato 1** "Piano Operativo" approvato, l'**Allegato 2** "Piano dei Fabbisogni", di cui al paragrafo 6.5 del Capitolato Tecnico Parte Generale (Allegato all'Accordo Quadro).

2.3 In particolare, per ogni condizione, modalità e termine per la prestazione dei servizi oggetto del presente Contratto Esecutivo che non sia espressamente regolata nel presente atto, vale tra le Parti quanto stabilito nell'Accordo Quadro, ivi inclusi gli Allegati del medesimo, con il quale devono intendersi regolati tutti i termini del rapporto tra le Parti.

2.4 Le Parti espressamente convengono che il predetto Accordo Quadro, ha valore di regolamento e pattuizione per il presente Contratto esecutivo. Pertanto, in caso di contrasto tra i principi dell'Accordo Quadro e quelli del Contratto esecutivo, i primi prevarranno su questi ultimi, salvo diversa espressa volontà derogativa delle parti manifestata per iscritto.

3. OGGETTO DEL CONTRATTO ESECUTIVO

3.1 Il presente Contratto esecutivo definisce i termini e le condizioni che, unitamente alle disposizioni contenute nell'Accordo Quadro, regolano la prestazione in favore

dell'Amministrazione da parte del Fornitore dei seguenti servizi: _____, come riportati nel Piano Operativo approvato di cui all'Allegato 1 e nel Piano dei Fabbisogni di cui all'Allegato 2 al presente documento.

3.2 I predetti servizi dovranno essere erogati con le modalità ed alle condizioni stabilite nel presente Contratto esecutivo e nell'Accordo Quadro e relativi allegati.

3.3 È designato quale Responsabile unico del procedimento ai sensi dell'art. 31 del D.Lgs. n. 50/2016 e Direttore dell'esecuzione, ai sensi dell'art. 101 del D. Lgs. n. 50/2016, il Dott. _____. <*in alternativa*: Sono designati quale Responsabile unico del procedimento, ai sensi dell'art. 31 del D. Lgs. n. 50/2016 il Dott. _____ e Direttore dell'esecuzione ai sensi dell'art. 101 del D. Lgs. n. 50/2016 il Dott. _____>.

3.4 L'affidatario si impegna a rispettare tutti i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale in ottemperanza al principio di non arrecare un danno significativo all'ambiente "Do No Significant Harm" (DNSH), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.

3.5 *<In caso di Contratto esecutivo affidato da un Soggetto Aggregatore, indicare tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'Affidamento>.*

4. EFFICACIA E DURATA

4.1 Il presente Contratto esecutivo spiega i suoi effetti dalla data della sua sottoscrizione ed avrà termine allo spirare di _____ <*indicare la durata contrattuale in ragione di quanto previsto al par. 2 del Capitolato Tecnico Generale>* mesi dalla data di conclusione delle attività di presa in carico.

4.2 Le Amministrazioni possono, nei limiti di quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016, chiedere al Fornitore prestazioni supplementari rispetto al Contratto esecutivo, che si rendano necessarie, ove un cambiamento del contraente produca entrambi gli effetti di cui all'art. 106, comma 1, lettera b), D. Lgs. n. 50/2016; l'Amministrazione comunicherà ad ANAC tale modifica entro i termini di cui all'art. 106, comma 8, del medesimo decreto.

4.3 Le Amministrazioni possono apportare modifiche al contratto esecutivo ove siano soddisfatte tutte le condizioni di cui all'art. 106, comma 1, lettera c), D. Lgs. 50/2016, fatto salvo quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016. Al ricorrere delle condizioni di cui all'art. 106, comma 14, del D. Lgs. 50/2016 l'Amministrazione comunicherà ad ANAC tale modifica entro i termini e con le modalità ivi indicati. In entrambi i casi sopra descritti, l'Amministrazione eseguirà le pubblicazioni prescritte dall'art. 106, comma 5, del D. Lgs. n. 50/2016.

4.4 Le Amministrazioni potranno apportare le modifiche di cui art. 106, comma 1, lett. d), del D. Lgs. n. 50/2016, nel pieno rispetto di tale previsione normativa.

4.5 Ai sensi dell'art. 106, comma 12, del D.Lgs. n. 50/2016, ove ciò si renda necessario in corso di esecuzione, l'Amministrazione potrà imporre al Fornitore affidatario del Contratto esecutivo un aumento o una diminuzione delle prestazioni fino a concorrenza di un quinto dell'importo del contratto alle stesse condizioni ed agli stessi prezzi unitari previsti nel presente contratto. In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.

5. GESTIONE DEL CONTRATTO ESECUTIVO

5.1 Ai fini dell'esecuzione del presente Contratto esecutivo, il Fornitore ha nominato come Responsabile Unico delle Attività Contrattuali (RUAC) e come Referente/i Tecnico/i per l'erogazione dei servizi: il/i dott._____

5.2 I compiti demandati alle suddette figure del Fornitore sono declinati al paragrafo 7.2 del Capitolato Tecnico Generale dell'Accordo Quadro.

5.3 Le attività di supervisione e controllo della corretta esecuzione del presente Contratto esecutivo, in relazione ai servizi richiesti, sono svolte dall'Amministrazione, eventualmente d'intesa con i soggetti indicati nell'Allegato Governance al Capitolato Tecnico Generale dell'Accordo Quadro.

6. PRESA IN CARICO E TRASFERIMENTO DEL KNOW HOW

6.1 Il Fornitore, a decorrere dalla data di stipula del presente Contratto esecutivo, dovrà procedere alla attività di presa in carico con le modalità indicate nel Capitolato Tecnico Speciale dell'Accordo Quadro.

6.2 L'attivazione dei servizi avverrà nei tempi e nei modi di cui al Capitolato Tecnico Generale e Speciale dell'Accordo Quadro, al Piano dei Fabbisogni ed al Piano Operativo.

6.3 In base ai servizi richiesti da parte dell'Amministrazione contraente, alla scadenza del presente Contratto esecutivo o in caso di risoluzione o recesso dallo stesso, il Fornitore si impegna a porre in essere tutte le attività per il passaggio di consegne di fine fornitura (phase-out), finalizzato al trasferimento all'Amministrazione, o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione delle attività, secondo quanto previsto nel paragrafo 4.3 del Capitolato Tecnico Speciale (2B).

7. LOCALI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE CONTRAENTE

7.1 L'Amministrazione Contraente provvede ad indicare e mettere a disposizione del Fornitore, in comodato gratuito ed in uso non esclusivo, locali idonei alla installazione degli eventuali apparati del Fornitore necessari all'erogazione dei servizi richiesti, con le modalità indicate nel Piano dei Fabbisogni e nel Piano Operativo.

7.2 L'Amministrazione Contraente garantisce al Fornitore:

- lo spazio fisico necessario per l'alloggio delle apparecchiature ed idoneo ad ospitare le apparecchiature medesime;
- l'alimentazione elettrica delle apparecchiature di adeguata potenza; sarà cura del Fornitore provvedere ad adottare ogni misura per la garantire la continuità della alimentazione elettrica.

7.3 Il Fornitore provvede a visitare i locali messi a disposizione dall'Amministrazione Contraente ed a segnalare, prima della data di disponibilità all'attivazione, l'eventuale inidoneità tecnica degli stessi.

7.4 L'Amministrazione Contraente consentirà al personale del Fornitore o a soggetti da esso indicati, muniti di documento di riconoscimento, l'accesso ai propri locali per eseguire eventuali operazioni rientranti nell'oggetto del presente Contratto esecutivo. Le modalità dell'accesso saranno concordate fra le Parti al fine di salvaguardare la legittima esigenza

di sicurezza dell'Amministrazione Contraente. Il Fornitore è tenuto a procedere allo sgombero, a lavoro ultimato, delle attrezzature e dei materiali residui.

7.5 L'Amministrazione Contraente, successivamente all'esito positivo delle verifiche di conformità a fine contratto, porrà in essere quanto possibile affinché gli apparati del Fornitore presenti nei suoi locali non vengano danneggiati o manomessi, pur non assumendosi responsabilità se non quelle derivanti da dolo o colpa grave del proprio personale.

8. VERIFICHE DI CONFORMITA'

8.1 Nel periodo di efficacia del presente Contratto esecutivo, ciascuna Amministrazione Contraente procederà ad effettuare la verifica di conformità delle prestazioni oggetto di ciascun Contratto esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali, con le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico Generale e Speciale ad esso allegati.

9. PENALI

9.1 L'Amministrazione potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nell'Accordo Quadro, qui da intendersi integralmente trascritte.

9.2 Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 12 dell'Accordo Quadro.

10. CORRISPETTIVI

10.1 Il corrispettivo complessivo, calcolato sulla base del dimensionamento dei servizi indicato del Piano dei Fabbisogni e nel Piano Operativo, è pari a <*inserire importo in cifre*> € _____,___ <*eventuale*> così suddiviso _____.

10.2 I corrispettivi unitari per singolo servizio, dovuti al Fornitore per la fornitura dei servizi prestati in esecuzione del presente Contratto esecutivo sono determinati in ragione dei prezzi unitari stabiliti nell'Allegato "C" all'Accordo Quadro "Corrispettivi e Tariffe".

10.3 Il corrispettivo contrattuale si riferisce alla esecuzione dei servizi a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.
<nel caso di Contratto Esecutivo affidato da un Soggetto Aggregatore, dovranno essere indicati gli importi e i quantitativi relativi ad ogni singola Amministrazione>

10.4 I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore medesimo di ogni relativo rischio e/o alea. Il Fornitore non potrà vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.

10.5 Tali corrispettivi sono dovuti dall'Amministrazione Contraente al Fornitore a decorrere dalla "Data di accettazione" della fornitura e successivamente all'esito positivo della verifica di conformità della singola prestazione.

11. FATTURAZIONE E PAGAMENTI

11.1 La fattura relativa ai corrispettivi maturati secondo quanto previsto al precedente art. 10

viene emessa ed inviata dal Fornitore con cadenza _____.

11.2 Ciascuna fattura dovrà essere emessa nel rispetto di quanto prescritto nell'Accordo Quadro.

<nel caso di Contratto Esecutivo affidato da un Soggetto Aggregatore, dovranno essere indicate le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni>

11.3 Nel caso in cui risulti aggiudicatario del Contratto un R.T.I., le singole Società costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione, potranno provvedere ciascuna alla fatturazione "pro quota" delle attività effettivamente prestate. Le Società componenti il Raggruppamento potranno fatturare solo le attività effettivamente svolte, corrispondenti alla ripartizione delle attività. La società mandataria del Raggruppamento medesimo è obbligata a trasmettere, in maniera unitaria e previa predisposizione di apposito prospetto riepilogativo delle attività e delle competenze maturate, le fatture relative all'attività svolta da tutte le imprese raggruppate. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi / attività / fasi / prodotti a cui si riferisce.

11.4 I corrispettivi saranno accreditati, a spese del Fornitore, sul conto corrente n. _____, intestato al Fornitore presso _____, Codice IBAN _____; il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i all'Amministrazione all'atto del perfezionamento del presente Contratto Esecutivo.

11.5 Ove applicabile in funzione della tipologia di prestazioni, ai sensi dell'art. 35, comma 18, del Codice, così come novellato dal D.L. 32/2019, il fornitore può ricevere, entro 15 giorni dall'effettivo inizio della/e prestazione/i contrattuali un'anticipazione del prezzo di ciascun Contratto Esecutivo pari al 20 per cento del valore del Contratto Esecutivo stesso. L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore dell'Amministrazione Contraente beneficiaria della prestazione, rilasciata dai soggetti indicati all'art. 35, comma 18, del Codice, di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma (o altro documento equivalente tipo SLA) della prestazione che indicato nel Capitolato Tecnico relativo all'Appalto Specifico

11.6 L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento della/e prestazione/i, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.

11.7 Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione della/e prestazione/i, non procede, per ritardi a lui imputabili, secondo il cronoprogramma concordato. Sulle somme restituite sono dovuti gli interessi legali con decorrenza dalla data di erogazione dell'anticipazione.

12. GARANZIA DELL'ESATTO ADEMPIMENTO

12.1 Il Fornitore ha prestato garanzia definitiva rilasciata in data _____ dalla _____ avente n. _____ di importo pari ad Euro _____= (_____/00) che copre le

obbligazioni assunte con il presente contratto, il risarcimento dei danni derivanti dall'eventuale inadempimento delle stesse obbligazioni, nonché il rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'appaltatore, nonché, ove esistente, le obbligazioni assunte con il Patto di integrità.

12.2 L'Amministrazione ha inoltre il diritto di valersi della garanzia definitiva, nei limiti dell'importo massimo garantito: i) per l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione del contratto disposta in danno dell'esecutore; ii) per provvedere al pagamento di quanto dovuto dal Fornitore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene eseguito il contratto ed addetti all'esecuzione dell'appalto.

12.3 L'Amministrazione ha diritto di incamerare la garanzia, in tutto o in parte, per i danni che essa affermi di aver subito, senza pregiudizio dei suoi diritti nei confronti del Fornitore per la rifusione dell'ulteriore danno eventualmente eccedente la somma incamerata.

12.4 La garanzia prevede espressamente la rinuncia della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, nonché l'operatività della garanzia medesima entro 15 giorni, a semplice richiesta scritta.

12.5 Il Fornitore si impegna a tenere valida ed efficace la garanzia, mediante rinnovi e proroghe, per tutta la durata del presente contratto e, comunque, sino al perfetto adempimento delle obbligazioni assunte in virtù del presente contratto, pena la risoluzione di diritto del medesimo.

12.6 L'Amministrazione può richiedere al Fornitore la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte entro il termine di 10 (dieci) giorni dalla richiesta; in caso di inottemperanza, l'Amministrazione conseguirà la reintegrazione trattenendo quanto necessario dai corrispettivi dovuti al Fornitore.

12.7 La garanzia sarà progressivamente svincolata a misura dell'avanzamento dell'esecuzione contrattuale, nel limite massimo dell'80 per cento dell'iniziale importo garantito, secondo quanto stabilito dall'art. 103, comma 5, del D. Lgs. n. 50/2016, previa deduzione di crediti dell'Amministrazione verso il Fornitore e subordinatamente alla preventiva consegna, da parte del Fornitore all'Istituto garante, di un documento, in originale o copia autentica, attestante l'avvenuta esecuzione delle prestazioni contrattuali. Tale documento è emesso periodicamente dall'Amministrazione in ragione delle verifiche di conformità svolte. Il fornitore dovrà inviare per conoscenza all'Amministrazione la comunicazione che invia al Garante ai fini dello svincolo. Il Garante dovrà comunicare all'Amministrazione il valore dello svincolo. L'Amministrazione si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.

12.8 L'ammontare residuo della garanzia definitiva deve permanere fino alla data di emissione del certificato di verifica di conformità attestante la corretta esecuzione del Contratto esecutivo.

12.9 Resta fermo tutto quanto previsto dall'art. 103 del D. Lgs. n. 50/2016.

13. SUBAPPALTO *<OVE PREVISTO>*

13.1 L'Impresa si è riservata di affidare in subappalto, nella misura di_____, l'esecuzione delle seguenti prestazioni: _____ , salvo quanto previsto dall'art. 105, comma 12, del d. lgs. n. 50/2016.

13.2 L'Impresa si impegna a depositare presso Consip S.p.A., almeno venti giorni prima della data di effettivo inizio dell'esecuzione delle attività oggetto del subappalto: i) l'originale o la copia autentica del contratto di subappalto che deve indicare puntualmente l'ambito operativo del subappalto sia in termini prestazionali che economici; ii) dichiarazione attestante il possesso da parte del subappaltatore dei requisiti richiesti dalla documentazione di gara, per lo svolgimento delle attività allo stesso affidate, ivi inclusi i requisiti di ordine generale di cui all'articolo 80 del D. Lgs. n. 50/2016; iii) dichiarazione dell'appaltatore relativa alla sussistenza o meno di eventuali forme di controllo o collegamento a norma dell'art. 2359 c.c. con il subappaltatore; se del caso, v) documentazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione/certificazione prescritti dal D. Lgs. n. 50/2016 per l'esecuzione delle attività affidate.

13.3 In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, Consip S.p.A. procederà a richiedere al Fornitore l'integrazione della suddetta documentazione. Resta inteso che la suddetta richiesta di integrazione comporta l'interruzione del termine per la definizione del procedimento di autorizzazione del subappalto, che ricomincerà a decorrere dal completamento della documentazione.

13.4 I subappaltatori dovranno mantenere per tutta la durata del presente contratto, i requisiti richiesti per il rilascio dell'autorizzazione al subappalto. In caso di perdita dei detti requisiti Consip S.p.A. revocherà l'autorizzazione.

13.5 L'impresa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato nonché siano variati i requisiti di qualificazione o le certificazioni deve acquisire una autorizzazione integrativa.

13.6 Ai sensi dell'art. 105, comma 4, lett. a) del D. Lgs. n. 50/2016 e s.m.i. non sarà autorizzato il subappalto ad un operatore economico che abbia partecipato alla procedura di affidamento dell'Accordo Quadro.

13.7 Per le prestazioni affidate in subappalto: il subappaltatore, ai sensi dell'art. 105, comma 14, del Codice, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconoscere ai lavoratori un trattamento economico e normativo non inferiore a quello che avrebbe garantito il contraente principale, inclusa l'applicazione dei medesimi contratti collettivi nazionali di lavoro, qualora le attività oggetto di subappalto coincidano con quelle caratterizzanti l'oggetto dell'appalto ovvero riguardino le lavorazioni relative alle categorie prevalenti e siano incluse nell'oggetto sociale del contraente principale;

13.8 L'Amministrazione contraente, sentito il direttore dell'esecuzione, provvede alla verifica dell'effettiva applicazione degli obblighi di cui al presente comma. Il Fornitore è solidalmente responsabile con il subappaltatore degli adempimenti, da parte di questo ultimo, degli obblighi di sicurezza previsti dalla normativa vigente.

13.9 Il Fornitore e il subappaltatore sono responsabili in solido, nei confronti dell'Amministrazione Contraente, in relazione alle prestazioni oggetto del contratto di subappalto.

13.10 L'Impresa è responsabile in solido con il subappaltatore nei confronti dell'Amministrazione contraente dei danni che dovessero derivare ad essa o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività. In particolare, il Fornitore e il subappaltatore si impegnano a manlevare e tenere indenne la Consip e l'Amministrazione da qualsivoglia pretesa di terzi per fatti e colpe imputabili al subappaltatore o ai suoi ausiliari derivanti da qualsiasi perdita, danno, responsabilità, costo o spesa che possano originarsi da eventuali violazioni del Regolamento 679/2016.

13.11 Il Fornitore è responsabile in solido dell'osservanza del trattamento economico e normativo stabilito dai contratti collettivi nazionale e territoriale in vigore per il settore e per la zona nella quale si eseguono le prestazioni da parte del subappaltatore nei confronti dei suoi dipendenti, per le prestazioni rese nell'ambito del subappalto. Il Fornitore trasmette all'Amministrazione contraente prima dell'inizio delle prestazioni la documentazione di avvenuta denunzia agli enti previdenziali, inclusa la Cassa edile, ove presente, assicurativi e antinfortunistici, nonché copia del piano della sicurezza di cui al D. Lgs. n. 81/2008. Ai fini del pagamento delle prestazioni rese nell'ambito dell'appalto o del subappalto, la stazione appaltante acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.

13.12 Il Fornitore è responsabile in solido con il subappaltatore in relazione agli obblighi retributivi e contributivi, ai sensi dell'art. 29 del D. Lgs. n. 276/2003, ad eccezione del caso in cui ricorrano le fattispecie di cui all'art. 105, comma 13, lett. a) e c), del D. Lgs. n. 50/2016.

13.13 Il Fornitore si impegna a sostituire i subappaltatori relativamente ai quali apposita verifica abbia dimostrato la sussistenza dei motivi di esclusione di cui all'articolo 80 del D. Lgs. n. 50/2016.

13.14 L'Amministrazione Contraente corrisponde direttamente al subappaltatore, al cottimista, al prestatore di servizi ed al fornitore di beni o lavori, l'importo dovuto per le prestazioni dagli stessi eseguite nei seguenti casi: a) quando il subappaltatore o il cottimista è una microimpresa o piccola impresa; b) in caso di inadempimento da parte dell'appaltatore; c) su richiesta del subappaltatore e se la natura del contratto lo consente. In caso contrario, salvo diversa indicazione del direttore dell'esecuzione, il Fornitore si obbliga a trasmettere all'Amministrazione contraente entro 20 giorni dalla data di ciascun pagamento da lui effettuato nei confronti dei subappaltatori, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.

13.15 L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.

13.16 In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti commi, l'Amministrazione può risolvere il Contratto esecutivo, salvo il diritto al risarcimento del danno.

13.17 Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016, il Fornitore si obbliga a comunicare all'Amministrazione il nome del subcontraente, l'importo del contratto, l'oggetto delle prestazioni affidate.

13.18 Il Fornitore si impegna a comunicare all'Amministrazione, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione del contratto, il nome del sub-contraente, l'importo del sub-contratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto.

13.19 Non costituiscono subappalto le fattispecie di cui al comma 3 dell'art. 105 del d. lgs. n. 50/2016 e s.m.i.. Nel caso in cui l'Impresa intenda ricorrere alle prestazioni di soggetti terzi in forza di contratti continuativi di cooperazione, servizio e/o fornitura gli stessi devono essere stati sottoscritti in epoca anteriore all'indizione della procedura finalizzata all'aggiudicazione del contratto e devono essere consegnati all'Amministrazione prima o contestualmente alla sottoscrizione del Contratto.

13.20 Per tutto quanto non previsto si applicano le disposizioni di cui all'art. 105 del D.Lgs. 50/2016.

13.21 Restano fermi tutti gli obblighi e gli adempimenti previsti dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973 nonché dai successivi regolamenti.

13.22 L'Amministrazione provvederà a comunicare al Casellario Informatico le informazioni di cui alla Determinazione dell'Autorità di Vigilanza sui Contratti Pubblici (ora A.N.AC) n. 1 del 10/01/2008.

14. *<EVENTUALE>* CONDIZIONI E TEST RICHIESTI DAL CVCN

<Eventuale inserire condizioni/test in considerazione del riscontro del CVCN ai sensi dell'art. 1, comma 6, Legge n. 133/2019>

15. RISOLUZIONE E RECESSO

15.1 Le ipotesi di risoluzione del presente Contratto esecutivo e di recesso sono disciplinate, rispettivamente, agli artt. 14 e 15 dell'Accordo Quadro, cui si rinvia, nonché agli artt. "SUBAPPALTO" "TRASPARENZA DEI PREZZI", "TRACCIABILITÀ DEI FLUSSI FINANZIARI" e "TRATTAMENTO DEI DATI PERSONALI" del presente Documento.

15.2 *<Eventuale inserire le ipotesi di risoluzione o sospensione in accordo con quanto previsto nel precedente articolo 14>*

16. FORZA MAGGIORE

16.1 Nessuna Parte sarà responsabile per qualsiasi perdita che potrà essere patita dall'altra Parte a causa di eventi di forza maggiore (che includono, a titolo esemplificativo, disastri naturali, terremoti, incendi, fulmini, guerre, sommosse, sabotaggi, atti del Governo, autorità giudiziarie, autorità amministrative e/o autorità di regolamentazione indipendenti) a tale Parte non imputabili.

16.2 Nel caso in cui un evento di forza maggiore impedisca la prestazione dei servizi da parte del Fornitore, l'Amministrazione, impregiudicato qualsiasi diritto ad essa spettante in base alle disposizioni di legge sull'impossibilità della prestazione, non dovrà pagare i corrispettivi per la prestazione dei servizi fino a che i servizi non siano ripristinati e, ove

possibile, avrà diritto di affidare l'erogazione dei servizi in questione ad altro fornitore assegnatario per una durata ragionevole secondo le circostanze.

16.3 L'Amministrazione si impegna, inoltre, in tale eventualità a compiere le azioni necessarie al fine di risolvere tali accordi, non appena il Fornitore le comunichi di essere in grado di erogare nuovamente i servizi.

17. RESPONSABILITA' CIVILE *<eventuale>* E POLIZZA ASSICURATIVA

17.1 Fermo restando quanto previsto dall'Accordo Quadro, il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

<ove prevista>

17.2 A fronte dell'obbligo di cui al precedente comma, il Fornitore ha presentato polizza/e assicurativa/e conforme/i ai requisiti indicati nella Richiesta di Offerta (conformi all'allegato di gara dell'AQ).

17.3 Resta ferma l'intera responsabilità del Fornitore anche per danni coperti o non coperti e/o per danni eccedenti i massimali assicurati dalle polizze di cui al precedente comma 2.

17.4 Con specifico riguardo al mancato pagamento del premio, ai sensi dell'art. 1901 del c.c., l'Amministrazione si riserva la facoltà di provvedere direttamente al pagamento dello stesso, entro un periodo di 60 giorni dal mancato versamento da parte del Fornitore ferma restando la possibilità dell'Amministrazione di procedere a compensare quanto versato con i corrispettivi maturati a fronte delle attività eseguite.

17.5 Qualora il Fornitore non sia in grado di provare in qualsiasi momento la piena operatività delle coperture assicurative di cui al precedente comma 2 e qualora l'Amministrazione non si sia avvalsa della facoltà di cui al precedente comma 4, il Contratto potrà essere risolto di diritto con conseguente ritenzione della garanzia prestata a titolo di penale e fatto salvo l'obbligo di risarcimento del maggior danno subito.

17.6 Resta fermo che il Fornitore si impegna a consegnare, annualmente e con tempestività, all'Amministrazione, la quietanza di pagamento del premio, atta a comprovare la validità della polizza assicurativa prodotta per la stipula del contratto o, se del caso, la nuova polizza eventualmente stipulata, in relazione al presente contratto.

18. TRASPARENZA DEI PREZZI

18.1 L'Impresa espressamente ed irrevocabilmente:

a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione del presente contratto;

b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le Imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione del contratto stesso;

c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del

presente contratto rispetto agli obblighi con esse assunti, né a compiere azioni comunque volte agli stessi fini;

d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.Lgs. n. 50/2016 al fine di evitare situazioni di conflitto d'interesse.

18.2 Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma per tutta la durata del contratto lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'art. 1456 cod. civ., per fatto e colpa del Fornitore, che sarà conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione e con facoltà della Committente di incamerare la garanzia prestata.

19. ONERI FISCALI E SPESE CONTRATTUALI

19.1 Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto, come previsto all'art. 28 dell'Accordo Quadro.

19.2 Così come previsto dall'art. 29 del Accordo Quadro, ai sensi dell'art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010. Pertanto, le Amministrazioni Beneficiarie sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del presente Contratto esecutivo, il predetto contributo nella misura prevista dall'art. 2, lettera a) (8 per mille del valore del contratto esecutivo sottoscritto se non superiore ad € 1.000.000,00) o lettera b) (5 per mille del valore del contratto esecutivo sottoscritto se superiore ad € 1.000.000,00), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del presente Contratto Esecutivo.

19.3 Il valore complessivo del presente Contratto Esecutivo è quello espressamente indicato al precedente paragrafo 10.1. Di conseguenza, il valore del contributo dovuto dall'Amministrazione Beneficiaria ammonta ad €_____(Euro_____).

19.4 In caso di incremento (entro il 20% dell'importo iniziale) del valore del Contratto esecutivo a seguito di una modifica del Piano dei Fabbisogni e del Piano Operativo approvato dall'Amministrazione Beneficiaria ai sensi dell'articolo 6 dell'Accordo Quadro, quest'ultima è tenuta a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall'art. 2, lettera c) (3 per mille sull'incremento tra il valore del contratto esecutivo ed il valore dell'atto aggiuntivo), del D.P.C.M. 23 giugno 2010.

A tal fine, nei casi di cui al precedente periodo, il Fornitore provvederà a comunicare all'Amministrazione e per conoscenza a Consip, entro il termine di 10 (dieci) giorni solari dalla data di approvazione del Piano Operativo incrementato, il valore aggiornato del Piano Operativo e il valore del contributo dovuto in ragione del relativo incremento.

19.5 Il pagamento del contributo, deve essere effettuato tramite bonifico bancario sul seguente IBAN: Banca: Intesa San Paolo - IBAN: IT 27 X 03069 05036 100000004389

Detti contributi sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972 e pertanto non è prevista nessuna emissione di fattura; gli stessi non rientrano nell'ambito di applicazione della tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136.

20. TRACCIABILITÀ DEI FLUSSI FINANZIARI

20.1 Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.

20.2 Ferme restando le ulteriori ipotesi di risoluzione previste dal presente contratto, si conviene che l'Amministrazione, in ottemperanza a quanto disposto dall'art. 3, comma 9 bis della Legge 13 agosto 2010 n. 136, senza bisogno di assegnare previamente alcun termine per l'adempimento, potrà risolvere di diritto il presente contratto ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa con raccomandata a/r qualora le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136.

20.3 Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, secondo periodo della Legge 13 agosto 2010 n. 136, ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136.

20.4 Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui alla norma sopra richiamata è tenuto a darne immediata comunicazione all'Amministrazione e la Prefettura – Ufficio Territoriale del Governo della provincia ove ha sede l'Amministrazione.

20.5 Il Fornitore, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari.

20.6 L'Impresa è tenuta a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i qualsivoglia variazione intervenuta in ordine ai dati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il codice fiscale delle persone delegate ad operare su detto/i conto/i.

20.7 Ai sensi della Determinazione dell'AVCP (ora A.N.AC.) n. 10 del 22 dicembre 2010, il Fornitore, in caso di cessione dei crediti, si impegna a comunicare il/i CIG/CUP al cessionario, eventualmente anche nell'atto di cessione, affinché lo/gli stesso/i venga/no riportato/i sugli strumenti di pagamento utilizzati. Il cessionario è tenuto ad utilizzare conto/i corrente/i dedicato/i, nonché ad anticipare i pagamenti al Fornitore mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i del Fornitore medesimo riportando il CIG/CUP dallo stesso comunicato.

21. FORO COMPETENTE

21.1 Per tutte le questioni relative ai rapporti tra il Fornitore e l'Amministrazione, la competenza è determinata in base alla normativa vigente.

22. TRATTAMENTO DEI DATI PERSONALI

<specificare, nella Piano dei Fabbisogni e nei rispettivi documenti allegati, un sufficiente dettaglio sul contesto tecnologico e procedurale nel quale il Fornitore dovrà operare, anche con specifico riferimento alle misure tecniche e organizzative necessarie per garantire il rispetto degli obblighi di cui all'art. 32 del regolamento UE, coordinando tali informazioni con quanto indicato nell'atto di nomina del Fornitore a Responsabile del trattamento >

22.1 Con la sottoscrizione del presente contratto il Fornitore è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito anche "Normativa in tema di trattamento dei dati personali") e delle istruzioni nel seguito fornite.

22.2 Il Fornitore/Responsabile ha presentato garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.

22.3 Le finalità del trattamento sono: _____ (motivi per cui il fornitore tratta i dati) <*Valorizzare in ragione dell'oggetto del contratto*>

22.4 Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati comuni (es. dati anagrafici e di contatto ecc..) ; ii) dati sensibili (dati sanitari, opinioni politiche ecc.); iii) dati giudiziari. <*Valorizzare in ragione dell'oggetto del contratto*>

22.5 Le categorie di interessati sono: es. dipendenti e collaboratori, utenti dei servizi, ecc… <*Valorizzare in ragione dell'oggetto del contratto*>

22.6 Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
- ricevano la formazione necessaria in materia di protezione dei dati personali;
- trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default).

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive < *si precisa che tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato o includa il trattamento di dati sensibili di cui all'articolo 9, paragrafo 1, o i dati giudiziari di cui all'articolo 10*>, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE.

22.7 Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso <*personalizzare in ragione dell'oggetto del contratto*>:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

22.8 1) (Autorizzazione generale) Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente il Titolare del trattamento di ogni nomina e/o sostituzione dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.

<*Oppure*> 2) (Autorizzazione specifica) Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento. Nel caso in cui per le prestazioni del Contratto che comportano il trattamento di dati personali il Fornitore/ Responsabile ricorra a subappaltatori o subcontraenti è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al titolare.

Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà al Fornitore/Responsabile Inziale del trattamento la penale di cui all'Accordo Quadro e diffiderà lo stesso a far adottar al sub-Responsabile del trattamento tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, la Committente potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno;

Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata

dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori.

22.9 Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 23 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.

22.10 Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile del trattamento e/o di suoi sub-Responsabili.

22.11 Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto;

22.12 Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà la penale di cui all'Accordo Quadro e diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, la Committente potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

22.13 Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

22.14 Al termine della prestazione dei servizi oggetto del contratto, il Responsabile su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili

eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

22.15 Il Responsabile si impegna a attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema".

22.16 In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.

22.17 Su richiesta del Titolare, il Responsabile si impegna ad adottare, nel corso dell'esecuzione del Contratto, ulteriori garanzie quali l'applicazione di un codice di condotta approvato o di un meccanismo di certificazione approvato di cui agli articoli 40 e 42 del Regolamento UE, quando verranno emanati. L'Amministrazione potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

22.18 Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

22.19 Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.

22.20 Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

22.21 Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

Letto, approvato e sottoscritto
Roma, lì _____

_____	_____
(per l'Amministrazione)	(per il Fornitore)

Ai sensi e per gli effetti dell'art. 1341 c.c. il Fornitore dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti: Art. 1 Definizioni, Art. 3 Oggetto del Contratto esecutivo, Art. 4 Efficacia e durata, Art. 5 Gestione del Contratto esecutivo, Art. 6 Presa in carico e trasferimento del Know How, Art. 7 Locali messi a disposizione dell'Amministrazione contraente, Art. 8 Verifiche di conformità, Art. 9 Penali, Art. 10 Corrispettivi, Art. 11 Fatturazione e pagamenti, Art. 12 Garanzia dell'esatto adempimento, *<ove previsto>,* Art. 13 Subappalto, *<ove previsto>,* Art. 14 Condizioni e Test richiesti dal CVCN, Art. 15 Risoluzione e Recesso, Art. 16 Forza Maggiore, Art. 17 Responsabilità civile *<ove prevista>* e polizza assicurativa, Art. 18 Trasparenza dei prezzi, Art. 19 Oneri fiscali e spese contrattuali, Art. 20 Tracciabilità dei flussi finanziari Art. 21 Foro competente, Art. 22 Trattamento dei dati personali

Letto, approvato e sottoscritto

Roma, lì

_____

(per il Fornitore)