CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

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

ACCORDO QUADRO PER L'AFFIDAMENTO SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI AI SENSI DELL'ART. ex art. 54, co. 4 lett. a) DEL d.lgs. N. 50/2016

LOTTO 2

ID SIGEF 2296

SCHEMA DI ACCORDO QUADRO

PER L'AFFIDAMENTO SERVIZI DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

TRA

Consip S.p.A., a socio unico, con sede legale in Roma, Via Isonzo n. 19/E, capitale sociale Euro 5.200.000,00= i.v., iscritta al Registro delle Imprese presso la Camera di Commercio di Roma al n.REA 878407 di Roma, CF e P. IVA 05359681003, in persona dell'Amministratore Delegato e legale rappresentante, Ing. Cristiano Cannarsa, domiciliato per la carica presso la sede sociale, giusta poteri allo stesso conferiti dalla deliberazione di aggiudicazione del Consiglio di Amministrazione del 25/01/2022 (nel seguito per brevità anche "**Consip S.p.A**.")

E

- **Intellera Consulting S.r.l.**, sede legale in Milano, Piazza Tre Torri n. 2, capitale sociale Euro 1.500.000,00=, iscritta al Registro delle Imprese di Milano al n. 11088550964, P. IVA 11088550964, domiciliata ai fini del presente atto in Milano, Piazza Tre Torri n. 2, in persona dell'Amministratore Delegato e legale rappresentante Dott. Giancarlo Senatore, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti:
- **Teleconsys S.p.A.** con sede legale in Roma, Via Groenlandia n.31, capitale sociale Euro 300.000,00=, iscritta al Registro delle Imprese di Roma al n. 07059981006, P. IVA 07059981006, domiciliata ai fini del presente atto in Milano, Piazza Tre Torri n. 2;
- **H.S.P.I. S.p.A**., con sede legale in Bologna, Via Aldo Moro n. 16, capitale sociale Euro 220.000,00=, iscritta al Registro delle Imprese di Bologna al n. 02355801206, P. IVA 02355801206, domiciliata ai fini del presente atto in Milano, Piazza Tre Torri n. 2;
- **Capgemini Italia S.p.A. società soggetta a direzione e coordinamento di Capgemini S.E.**, con sede legale in Roma, Via di Torre Spaccata n. 140, capitale sociale Euro 27.734.459,00=, iscritta al Registro delle Imprese di Roma al n. 10365640159, P. IVA 16343831000, domiciliata ai fini del presente atto in Milano, Piazza Tre Torri n. 2;

giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott. Giovanni Vicini repertorio n. 227372 del 7 febbraio 2022;

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

PREMESSO

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, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, 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) che 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) che, 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) 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. 108 del 17/09/2021 e nella Gazzetta Ufficiale dell'Unione Europea n. S 178 del 14/09/2021, una procedura aperta per la stipula di un

Accordo Quadro, ai sensi dell'art. 54, comma 4, lett. a) del D. Lgs. n. 50/2016 con più operatori a condizione tutte fissate;

e) il Fornitore che sottoscrive il presente Accordo Quadro è risultato aggiudicatario della predetta procedura aperta per la quota PAC del Lotto 2 e, per l'effetto, ha manifestato la volontà di impegnarsi ad eseguire quanto stabilito nel presente Accordo Quadro e relativi Allegati alle condizioni, modalità e termini ivi stabiliti e nei successivi Contratti esecutivi;

f) che la stipula del presente Accordo Quadro con i suoi Allegati non è fonte di alcuna obbligazione per la Consip S.p.A. e/o per le Amministrazioni nei confronti del Fornitore;

g) che i singoli Contratti esecutivi verranno stipulati a tutti gli effetti tra le Amministrazioni PAC secondo l'indicazione di cui al par. 5 del Capitolato Tecnico Generale ed il Fornitore in base alle modalità ed i termini indicati nel presente Accordo Quadro e relativi Allegati;

h) che il Fornitore dichiara che quanto risulta dal presente Accordo Quadro e dai suoi Allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico (Generale e Speciale), nonché gli ulteriori atti della procedura, definisce in modo adeguato e completo gli impegni assunti con la firma del presente atto, nonché l'oggetto delle prestazioni da fornire e, in ogni caso, ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica delle stesse e per la formulazione dell'offerta;

i) il Fornitore ha presentato la documentazione richiesta ai fini della stipula del presente Accordo Quadro che, anche se non materialmente allegata al presente atto, ne forma parte integrante e sostanziale, ivi inclusa la garanzia definitiva nei confronti di Consip S.p.a., rilasciata dalla Coface ed avente n 2343646 per un importo di Euro 100.000,00=(centomila/00) a garanzia dell'adempimento delle obbligazioni contrattuali nascenti dall'Accordo Quadro;

j) che il Fornitore, con la seconda sottoscrizione, dichiara, ai sensi e per gli effetti di cui agli artt. 1341 e 1342 cod. civ., di accettare tutte le condizioni e patti contenuti nel presente Accordo Quadro e relativi Allegati, e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni riportate in calce al presente Accordo Quadro;

k) che il presente Accordo Quadro viene sottoscritto dalle parti con firma digitale rilasciata da ente certificatore autorizzato.

l) In data 25 febbraio 2022 è stato proposto dall'impresa NTT Data Italia S.p.A, innanzi al T.A.R. del Lazio, Roma, un giudizio iscritto al R.G. n. 2140/2022, contro Consip S.p.A e il RTI Deloitte Risk Advisory S.r.l. S.B., E&Y Advisory S.p.A., Teleco S.r.l. e nei confronti del RTI Intellera Consulting S.r.l., Cap Gemini Italia S.p.A., HSPI S.p.A. e Teleconsys S.p.A. per l'annullamento del provvedimento di aggiudicazione definitiva non efficace comunicato da Consip il 26/01/2022. Il Tar all'udienza camerale del 9/3/2022 non ha concesso misure cautelari ed in data 21/04/2022 ha pronunciato la sentenza n. 04840/2022 respingendo il gravame proposto da NTT Data Italia S.p.A..

Ciò premesso, tra le parti come in epigrafe rappresentate e domiciliate
SI CONVIENE E SI STIPULA QUANTO SEGUE

ARTICOLO 1 - DEFINIZIONI

1. Nell'ambito del presente Accordo Quadro, si intende per:

   a) **Accordo Quadro:** il presente atto, comprensivo di tutti i suoi Allegati, nonché dei documenti ivi richiamati, quale accordo concluso da Consip S.p.A. anche per conto delle Amministrazioni, da una parte, ed il Fornitore, dall'altra parte, con lo scopo di stabilire le clausole relative agli Contratti esecutivi da affidare per tutta la durata del

medesimo Accordo Quadro;

b) **Amministrazione/i o Amministrazione/i Contraente/i PAC:** le stazioni appaltanti, nonché gli altri soggetti che ai sensi della normativa vigente sono legittimati a affidare Contratti esecutivi basati sul presente Accordo Quadro secondo la classificazione di cui al par. 5 del Capitolato Tecnico Generale;

m) **Ministero:** Ministero dell'Economia e delle Finanze;

c) **Data di Attivazione**: la data a partire dalla quale le Amministrazioni Pubbliche possono utilizzare l'Accordo Quadro, ai sensi di quanto disposto nel successivo art. 4;

d) **Fornitore**: il singolo aggiudicatario (impresa, raggruppamento temporaneo o consorzio di imprese) della procedura aperta di cui in premessa, che, conseguentemente, sottoscrive l'Accordo Quadro impegnandosi a quanto nello stesso previsto e, in particolare, ad eseguire i singoli Contratti esecutivi;

e) **Capitolato d'Oneri**: il documento allegato al presente atto che ha disciplinato la partecipazione alla procedura aperta di cui in premessa, e contenente, altresì, le condizioni e le modalità per l'affidamento dei Contratti esecutivi;

f) **Contratto esecutivo:** il Contratto che si perfeziona in seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione del Piano operativo da parte dell'operatore economico, individuato, tra gli aggiudicatari dell'Accordo Quadro, avente ad oggetto l'affidamento di servizi di compliance e controllo, in base ai criteri, le modalità ed i termini indicati nel presente Accordo Quadro e nel paragrafo 6.5 del Capitolato Tecnico Generale;

g) **Piano dei Fabbisogni:** il documento inviato dall'Amministrazione al Fornitore, con il la stessa identifica e contestualizza i servizi oggetto del proprio Contratto esecutivo e nel quale dovranno essere riportate, tra le altre cose, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore;

h) **Piano operativo:** il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel Capitolato Tecnico Generale;

i) **Giorno lavorativo**: da lunedì a sabato, esclusi domenica e festivi;

j) **Soggetti aggregatori:** le centrali di committenza iscritte nell'elenco istituito ai sensi dell'art. 9, comma 1, del decreto legge 24 aprile 2014, n. 66, convertito con modificazioni, dalla legge 23 giugno 2014, n. 89, come definiti all'art. 3, comma 1, lett. n) del D.Lgs. n. 50/2016.

2. Le espressioni riportate negli Allegati al presente Accordo Quadro hanno il significato, per ognuna di esse, specificato nei medesimi Allegati, tranne qualora il contesto delle singole clausole dell'Accordo Quadro disponga diversamente.

ARTICOLO 2 - VALORE DELLE PREMESSE, DEGLI ALLEGATI E NORME REGOLATRICI

1. Le premesse di cui sopra, gli atti ed i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ivi incluso il Bando di gara, il Capitolato d'Oneri, il Capitolato Tecnico Generale e Speciale e le relative appendici, i chiarimenti resi in fase di gara, le Regole del Sistema di e-Procurement della Pubblica Amministrazione – Parte I, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Accordo Quadro. Tali documenti sono disponibili al seguente link: www.consip.it.
2. Costituiscono, altresì, parte integrante e sostanziale dell'Accordo Quadro: l'Allegato "**A**" (Offerta Tecnica del Fornitore), Allegato "**B**" (Offerta Economica del Fornitore) Allegato "**C**" (Corrispettivi e tariffe PAC) Allegato "**D**" (Patto di integrità), l'Allegato "**E**" (Nomina a responsabile del trattamento dei dati), l'Allegato **"F"** (Schema di contratto esecutivo – Lotto 2),), l'Allegato **"G"** (Disposizioni per la Governance), l'Allegato **"H"** (Regolamento degli organismi di coordinamento e controllo),l'Allegato "**I**" Contratto di avvalimento;
3. Il presente Accordo Quadro è regolato:

   a) dal contenuto dell'Accordo Quadro e dei suoi Allegati che costituiscono la manifestazione integrale di tutti gli accordi intervenuti con il Fornitore relativamente alle attività e prestazioni contrattuali che costituiscono parte integrante e sostanziale dell'Accordo Quadro;

b) dalle disposizioni di cui al D.Lgs. n. 50/2016 e s.m.i.;

c) dalle disposizioni di cui al d.P.R. 10 ottobre 2010, n. 207, nei limiti stabiliti dagli artt. 216 e 217 del D. Lgs. n. 50/2016;

d) dalle disposizioni anche regolamentari in vigore per le Amministrazioni, di cui il Fornitore dichiara di avere esatta conoscenza e che, sebbene non siano materialmente allegati, formano parte integrante del presente atto;

e) dalle norme in materia di Contabilità pubblica;

f) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato;

g) dal Codice Etico e dal Piano Triennale per la prevenzione della corruzione e della trasparenza della Consip S.p.A., consultabili sul sito internet della stessa Consip;

h) dal patto di integrità.

4. I Contratti esecutivi saranno regolati, dalle disposizioni in essi previste, dal presente Accordo Quadro e dai suoi allegati, dalle disposizioni indicate al precedente comma.
5. In caso di contrasto o difficoltà interpretativa tra quanto contenuto nel presente Accordo Quadro e relativi Allegati, da una parte, e quanto dichiarato nell'Offerta Tecnica, dall'altra parte, prevarrà quanto contenuto nei primi, fatto comunque salvo il caso in cui l'Offerta Tecnica contenga, a giudizio di Consip S.p.A. e/o delle Amministrazioni, previsioni migliorative rispetto a quelle contenute nel presente Accordo Quadro e relativi Allegati.
6. Le clausole dell'Accordo Quadro e dei Contratti esecutivi sono sostituite, modificate od abrogate automaticamente per effetto di norme aventi carattere cogente contenute in leggi o regolamenti che entreranno in vigore successivamente, fermo restando che in ogni caso, anche ove intervengano modificazioni autoritative dei prezzi migliorativi per il Fornitore, quest'ultimo rinuncia a promuovere azioni o ad opporre eccezioni rivolte a sospendere o a risolvere il rapporto contrattuale in essere.
7. Nel caso in cui dovessero sopraggiungere provvedimenti di pubbliche autorità dai contenuti non suscettibili di inserimento di diritto nel presente Accordo Quadro e nei Contratti esecutivi e che fossero parzialmente o totalmente incompatibili con l'Accordo Quadro e relativi Allegati e/o con i Contratti esecutivi, Consip S.p.A. e/o le Amministrazioni, da un lato, e il Fornitore, dall'altro lato, potranno concordare le opportune modifiche ai surrichiamati documenti sul presupposto di un equo contemperamento dei rispettivi interessi e nel rispetto dei relativi criteri di aggiudicazione della procedura.

ARTICOLO 3 - OGGETTO DELL'ACCORDO QUADRO

1. L'Accordo Quadro definisce la disciplina normativa e contrattuale relativa alle condizioni e alle modalità di affidamento da parte delle Amministrazioni dei singoli Contratti esecutivi aventi ad oggetto l'affidamento di servizi di compliance e controllo (Lotto 2 PAC) alle condizioni tutte espressamente stabilite nel presente atto e relativi Allegati.

   Il valore indicativo stimato dell'Accordo Quadro, rappresentativo della sommatoria dell'importo massimo presunto dei Contratti esecutivi che verranno affidati in virtù dell'Accordo Quadro medesimo, è il seguente: Euro 117.000.000,00 = (centodiciassettemilioni) IVA esclusa, come di seguito suddiviso:

   - attribuzione della quota massima del valore di Euro 46.800.000,00 = (quarantaseimilioniottocentomila), IVA esclusa, al Fornitore graduato secondo nella graduatoria di merito.

2. Qualora, anteriormente alla scadenza del termine di durata dell'Accordo Quadro, anche eventualmente prorogata, il valore relativo ad un Contratto esecutivo raggiunga il valore stimato dell'Accordo Quadro medesimo oppure lo ecceda (comunque fino a una soglia massima del 20%), Consip considererà quest'ultimo come giunto a scadenza e di conseguenza non potranno essere affidati ulteriori Contratti esecutivi. La regola sopra illustrata opera sul massimale della quota di AQ stipulato con il Fornitore.

3. Il presente Accordo Quadro è concluso con il Fornitore aggiudicatario della procedura aperta di cui in premessa, il quale con la sottoscrizione del presente atto, si impegna a dare esecuzione ai Contratti esecutivi che si perfezioneranno all'esito dell'approvazione del Piano operativo, quale affidamento in favore del Fornitore del Contratto esecutivo basato sulle condizioni stabilite nel presente Accordo Quadro e relativi Allegati.
4. L'affidamento del Contratto esecutivo da parte della singola Amministrazione avverrà in favore del Fornitore che sottoscrive il presente contratto in ragione del fatto che la medesima appartiene alla PAC come indicato al capitolo 5 del Capitolato Tecnico Generale.
5. Il Fornitore, pertanto, si impegna ad eseguire, in caso di affidamento dei singoli Contratti esecutivi, i servizi di compliance e controllo descritti nel Capitolato Tecnico Speciale (Lotto 2) secondo quanto ivi stabilito e nel rispetto delle condizioni di erogazione migliorative eventualmente offerte in sede di gara, nonché, in ogni caso nel rispetto di quanto stabilito nel Capitolato d'oneri, nel Capitolato Tecnico (Generale e Speciale) e negli atti della documentazione di gara, ovvero se migliorative, nell'Offerta Tecnica allegata.
6. Al fine di affidare un Contratto esecutivo basato sul presente Accordo Quadro, le singole Amministrazioni procedono:
   a) alla definizione dell'oggetto del singolo Contratto esecutivo, del quantitativo e dell'importo contrattuale, nel rispetto di quanto stabilito ed alle condizioni di cui al presente Accordo Quadro e relativi Allegati e comunque di quanto previsto al paragrafo 6.5 del Capitolato Tecnico Generale;
   b) <*qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Contratto esecutivo sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019*> alla comunicazione al CVCN o a uno dei CV secondo quanto previsto dall'art. 1 comma 6, legge n. 133/2019 la cui efficacia è stata modificata dall'art 16 comma 9, lett. a) della Legge n. 109/2021 secondo quanto previsto dall'art. 1 comma 6, legge n. 133/2019;
   c) all'affidamento del Contratto esecutivo in favore del Fornitore approvando il Piano Operativo nel rispetto delle condizioni previste nel presente Accordo Quadro e relativi Allegati, e al conseguente perfezionamento del relativo Contratto Esecutivo.

ARTICOLO 4 - DURATA DELL'ACCORDO QUADRO E DEI CONTRATTI ESECUTIVI

1. Il presente Accordo Quadro ha una durata di 24 mesi a decorrere dalla data di attivazione, ovvero la minore durata determinata dall'esaurimento del valore massimo stabilito nel precedente articolo.
2. Resta inteso che, per durata dell'Accordo Quadro, si intende il termine entro il quale le Amministrazioni potranno affidare i singoli Contratti esecutivi al Fornitore per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro stesso.
3. Ciascun Contratto esecutivo ha una durata massima di 48 mesi, decorrenti dalla data di conclusione delle attività di presa in carico.
4. L'Amministrazione, in conformità a quanto disposto all'articolo 106, comma 11, del D. Lgs. n. 50/2016, si riserva la facoltà in corso di esecuzione di modificare la durata del contratto, con comunicazione inviata a mezzo pec al Fornitore, prorogandolo per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione di un nuovo contraente, ivi inclusa la stipula del contratto. In tal caso il Fornitore è tenuto all'esecuzione delle prestazioni previste nel contratto agli stessi prezzi, patti e condizioni o più favorevoli per l'Amministrazione.

ARTICOLO 5 - PREZZI E VINCOLI DEI CONTRATTI ESECUTIVI

1. I corrispettivi per ciascun Contratto esecutivo verranno determinati sulla base dei prezzi stabiliti nell'Allegato **"C"**, "Corrispettivi e tariffe PAC", i quali rappresentano quindi un vincolo per il Fornitore.
2. Il Fornitore, inoltre, nel dare seguito al singolo Contratto esecutivo dovrà, fermi i prezzi unitari offerti, fornire servizi che dovranno necessariamente possedere tutte le caratteristiche (minime e migliorative offerte) per l'aggiudicazione del presente Accordo Quadro.
3. Il pagamento dei corrispettivi dovrà essere effettuato mediante strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché ai sensi delle emanate Determinazioni dell'A.N.AC., e, fatte salve le eventuali ulteriori indicazioni sugli "strumenti idonei" che dovessero essere emanate dalla medesima Autorità.
4. La disciplina della revisione dei corrispettivi dovuti al Fornitore sarà definita dalle Amministrazioni in sede di Contratto esecutivo, fermo restando quanto previsto all'art. 106 comma1 del D. Lgs. 50/2016.

ARTICOLO 6 - AFFIDAMENTO DEI CONTRATTI ESECUTIVI

1. Ciascun Contratto esecutivo verrà affidato dalla singola Amministrazione nel rispetto e alle condizioni stabilite al paragrafo 6.5 del capitolato Tecnico Generale, al paragrafo 24 del Capitolato d'Oneri e agli artt. 3 e 4 del presente atto.
2. Sono legittimate ad utilizzare il presente Accordo Quadro, ai sensi della normativa vigente, le Amministrazioni PAC come definite nel precedente articolo 1 e sulla base di quanto indicato al capitolo 5 del Capitolato Tecnico Generale ("Razionali per l'utilizzo dei Lotti"). Ove il Fornitore ritenga di non poter dare seguito al Contratto esecutivo, in quanto proveniente da un soggetto non legittimato sulla base di quanto sopra, dovrà, tempestivamente e comunque entro il termine stabilito al paragrafo 6.5.2. del Capitolato Tecnico Generale, informare Amministrazione e Consip, spiegando le ragioni del rifiuto.
3. All'esito della procedura di cui al paragrafo 6.5 del Capitolato Tecnico Generale, l'Amministrazione invierà a mezzo PEC al Fornitore il Piano operativo approvato ed il Contratto esecutivo sottoscritto.
4. Qualora il Fornitore rilevi eventuali difformità, nell'ambito del Contratto esecutivo, rispetto alle previsioni di cui al presente Accordo Quadro e relativi allegati e al Capitolato Tecnico Generale, ovvero la mancanza degli elementi essenziali dello schema di Contratto esecutivo, dovrà darne tempestiva comunicazione all'Amministrazione, entro e non oltre quattro giorni lavorativi dal ricevimento del Contratto esecutivo stesso. In tal caso, l'Amministrazione potrà trasmettere nuovamente il Contratto esecutivo, conforme alle previsioni di cui all'Accordo Quadro e relativi allegati.
5. In assenza di comunicazioni ai sensi del precedente comma 4, il singolo Contratto esecutivo si perfezionerà in ogni caso il quarto giorno lavorativo successivo alla trasmissione, da parte dell'Amministrazione, del Contratto esecutivo dalla stessa sottoscritto. Spirato il predetto termine, nonché in caso di accettazione espressa, il Fornitore sarà pertanto tenuto a dare esecuzione completa alla fornitura richiesta. Il ritardo nell'avvio dell'esecuzione per causa imputabile al Fornitore costituisce causa di risoluzione di diritto del Contratto esecutivo, ai sensi dell'art. 2, comma 1 della L. n. 120/2020 DL. 76/2020.
6. Per effetto del perfezionamento del Contratto esecutivo, il Fornitore sarà obbligato ad eseguire la fornitura richiesta, nell'ambito dell'oggetto contrattuale, restando inteso che in caso di mancata utilizzazione dell'Accordo Quadro da parte dei soggetti sopra indicati nulla potrà essere preteso a qualsiasi titolo dal medesimo Fornitore il quale, infatti, sarà tenuto a svolgere le attività, effettuare le forniture e prestare i servizi solo a seguito del perfezionamento dei Contratti esecutivi, con le modalità ed in conformità alle condizioni sopra indicate.
7. Resta inteso che Consip non potrà in alcun modo essere ritenuta responsabile per il mancato perfezionamento dei

Contratti esecutivi da parte delle Amministrazioni ed inoltre resta fermo che non sussiste in capo a Consip alcuna verifica dei poteri di acquisto attribuiti al sottoscrittore del Contratto esecutivo.

8. Qualora il Fornitore non abbia autorizzato Consip alla pubblicazione delle generalità e del codice fiscale del/i delegato/i ad operare sul conto/i corrente/i dedicato/i, il Fornitore medesimo sarà tenuto a comunicare, entro e non oltre due giorni dal perfezionamento del singolo Contratto esecutivo i surrichiamati dati alle Amministrazioni Contraenti.
9. Qualora venga richiesto da Consip, il Fornitore, entro un giorno lavorativo dalla richiesta, ha l'obbligo di dare riscontro alla medesima Consip, anche per via telematica, di ciascun Contratto esecutivo perfezionato.
10. Le Amministrazioni provvederanno, prima della sottoscrizione del singolo Contratto esecutivo, tra le altre cose: i) alla nomina del Responsabile del Procedimento, ai sensi e per gli effetti dell'art. 31 del D.Lgs. n. 50/2016 ii) alla nomina del Direttore dell'esecuzione, laddove le relative funzioni non siano svolte dal Responsabile del procedimento nel rispetto degli artt. 101, 102 e 111 del D.Lgs. n. 50/2016; iii) ai sensi e per gli effetti dell'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i., degli artt. 6 e 7 del Decreto Legge 12 novembre 2010, n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora A.N.AC.) n. 8 del 18 novembre 2010, alla indicazione sul medesimo Contratto esecutivo del CIG (Codice Identificativo Gara) "derivato" rispetto a quello dell'Accordo Quadro e da esse richiesto nonché del CUP (Codice Unico Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3.
11. Le Amministrazioni provvederanno, ove ritenuto necessario, alla nomina del Fornitore quale Responsabile o sub Responsabile del trattamento dei dati personali, eventualmente utilizzando l'Allegato Privacy, accluso al presente Accordo Quadro.
12. Resta salva la facoltà per Consip S.p.A. di svolgere controlli sull'esecuzione delle singole prestazioni.
13. Nel caso di Contratto esecutivo affidato da un Soggetto Aggregatore, nel Progetto dei fabbisogni il Soggetto Aggregatore, inoltre:
    - dovrà indicare tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'affidamento;
    - dovrà indicare gli importi e i quantitativi relativi ad ogni singola Amministrazione;
    - potrà indicare le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni.
14. Il Fornitore prende atto, rinunziando ora per allora a qualsiasi pretesa di risarcimento o di indennizzo, che l'Amministrazione ha la facoltà di revocare il Piano dei Fabbisogni, da esercitarsi entro un giorno lavorativo dall'emissione del medesimo.
15. 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.
16. 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.
17. 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.
18. Così come chiarito dal **Comunicato Anac del 23 marzo 2021**, l'Amministrazione potrà imporre al fornitore affidatario

dell'Appalto Specifico 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 dal presente Contratto, solo laddove ricorrano i presupposti di cui al **combinato disposto dei commi 1, lett. c) e 12 dell'art. 106, del Codice.** In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.

19. Per tutto quanto non espressamente previsto nel presente articolo, si applicano le disposizioni di cui all'art. 106 del D.Lgs. 50/2016.
20. Nel corso dell'esecuzione del Contratto esecutivo, l'Amministrazione potrà richiedere aggiornamenti del Piano dei Fabbisogni e del Piano Operativo ogni qualvolta lo ritenga necessario, nel rispetto delle previsioni di cui all'art. 106 del D.Lgs. 50/2016 nonché dell'importo massimo dell'Accordo Quadro.
21. Qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Contratto esecutivo sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019, atteso che prima di procedere all'affidamento del Contratto esecutivo, il Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 (convertito con modificazioni dalla L. 109/2021) presso l'Agenzia per la cybersicurezza nazionale, o uno dei Centri di Valutazione (CV), istituiti presso il Ministero dell'interno e il Ministero della difesa, potrà aver riscontrato la comunicazione della medesima prevedendo la necessità di effettuare verifiche preliminari e/o imporre condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2 lett. b) legge 133/2019, l'Amministrazione contraente prevedrà nel Contratto esecutivo medesimo le clausole che condizioneranno, sospensivamente ovvero risolutivamente al Contratto esecutivo al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.

ARTICOLO 7 - OBBLIGAZIONI GENERALI DEL FORNITORE

1. Sono a carico del Fornitore tutti gli oneri e rischi relativi alla prestazione delle attività oggetto dei Contratti esecutivi basati sul presente Accordo Quadro, nonché ad ogni attività che si rendesse necessaria per l'attivazione e la prestazione degli stessi o, comunque, opportuna per un corretto e completo adempimento delle obbligazioni previste, ivi compresi quelli relativi ad eventuali spese di trasporto, di viaggio e di missione per il personale addetto alla esecuzione contrattuale.
2. Il Fornitore si obbliga ad eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nell'Accordo Quadro, nel Capitolato d'Oneri, nel Capitolato Tecnico Generale e Speciale, nel Piano dei fabbisogni, nel Piano Operativo, ivi inclusi i rispettivi Allegati.
3. Le prestazioni contrattuali dovranno necessariamente essere conformi alle caratteristiche tecniche e qualitative eventualmente migliorate in Offerta tecnica ed alle specifiche indicate nel Capitolato d'Oneri e nei relativi Allegati; in ogni caso, il Fornitore si obbliga ad osservare, nell'esecuzione delle prestazioni contrattuali, tutte le norme e le prescrizioni tecniche e di sicurezza in vigore, nonché quelle che dovessero essere successivamente emanate.
4. Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula dell'Accordo Quadro, resteranno ad esclusivo carico del Fornitore, intendendosi in ogni caso remunerati con il corrispettivo contrattuale indicato nel Contratto esecutivo, ed il Fornitore non potrà, pertanto, avanzare pretesa di compensi a tale titolo, nei confronti delle Amministrazioni e/o della Consip S.p.A., assumendosene ogni relativa alea.
5. Il Fornitore si impegna espressamente a:

a) impiegare, a proprie cura e spese, tutte le strutture ed il personale necessario per l'esecuzione dei Contratti esecutivi secondo quanto specificato nell'Accordo Quadro e nei rispettivi Allegati e negli atti di gara richiamati nelle premesse;
b) rispettare, per quanto applicabili, le norme internazionali UNI EN ISO vigenti per la gestione e l'assicurazione della qualità delle proprie prestazioni;
c) predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a consentire alla Consip S.p.A. e alle singole Amministrazioni, per quanto di propria competenza, di monitorare la conformità dei servizi e delle forniture alle norme previste nell'Accordo Quadro e nei Contratti esecutivi fra i quali:
    i) l'invio entro il decimo giorno del mese successivo a quello di riferimento, dell'archivio in formato xml "FLUSSO DATI" recante i dati dei Contratti Esecutivi stipulati nel mese di riferimento;
    ii) l'Invio entro il 31 gennaio del 2023, 2024 e 2025, della relazione consuntiva "FATTURATO ANNUALE" contenente, per servizio e per Amministrazione, le quantità di servizi erogati, il fatturato e le penali applicate relativo all'anno precedente;
d) predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a garantire elevati livelli di servizio, ivi compresi quelli relativi alla sicurezza e riservatezza;
e) nell'adempimento delle proprie prestazioni ed obbligazioni, osservare tutte le indicazioni operative, di indirizzo e di controllo che a tale scopo saranno predisposte e comunicate dalle Amministrazioni o dalla Consip S.p.A., per quanto di rispettiva ragione;
f) comunicare tempestivamente a Consip S.p.A. e alle Amministrazioni, per quanto di rispettiva competenza, le eventuali variazioni della propria struttura organizzativa coinvolta nell'esecuzione dell'Accordo Quadro e nei singoli Contratti esecutivi, indicando analiticamente le variazioni intervenute ed i nominativi dei nuovi responsabili;
g) non opporre a Consip S.p.A. e alle Amministrazioni qualsivoglia eccezione, contestazione e pretesa relative alla fornitura e/o alla prestazione dei servizi;
h) manlevare e tenere indenne Consip S.p.A. e le Amministrazioni da tutte le conseguenze derivanti dalla eventuale inosservanza delle norme e prescrizioni tecniche, di sicurezza, di igiene e sanitarie vigenti;
i) adottare, in fase di esecuzione contrattuale, le eventuali cautele rese necessarie dallo svolgimento delle prestazioni affidate in locali o ambienti in cui l'Amministrazione Contraente tratta informazioni classificate, con particolare riguardo alle specifiche misure previste dalla normativa in proposito vigente;
j) rispettare gli obblighi in materia ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali elencate nell'allegato X del D. Lgs. n. 50/2016.
k) ad effettuare le verifiche preliminari richieste dal CVCN nonché a rispettare le condizioni e i test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2 lett. b) legge 133/2019 eventualmente imposti dal CVCN.

6. Le attività necessarie per la predisposizione dei mezzi e per l'attivazione dei servizi oggetto dell'Accordo Quadro e dei singoli Contratti esecutivi, eventualmente da svolgersi presso gli uffici delle Amministrazioni, dovranno essere eseguite senza interferire nel normale lavoro degli uffici; modalità e tempi dovranno comunque essere concordati con le Amministrazioni stesse nel rispetto di quanto stabilito nel Capitolato Tecnico Generale e Speciale; peraltro, il Fornitore prende atto che, nel corso dell'esecuzione delle prestazioni contrattuali, gli uffici delle Amministrazioni continueranno ad essere utilizzati dal personale delle Amministrazioni stesse e/o da terzi autorizzati. Il Fornitore si impegna, pertanto, ad eseguire le predette prestazioni salvaguardando le esigenze delle Amministrazioni e/o di terzi autorizzati, senza recare intralci, disturbi o interruzioni alla attività lavorativa in atto.

7. Il Fornitore rinuncia espressamente, ora per allora, a qualsiasi pretesa o richiesta di compenso nel caso in cui l'esecuzione delle prestazioni contrattuali dovesse essere ostacolata o resa più onerosa dalle attività svolte dalle Amministrazioni e/o da terzi autorizzati.
8. Il Fornitore si impegna ad avvalersi di personale specializzato, in relazione alle diverse prestazioni contrattuali; detto personale potrà accedere agli uffici delle Amministrazioni nel rispetto di tutte le relative prescrizioni di accesso, fermo restando che sarà cura ed onere del Fornitore verificare preventivamente tali procedure.
9. Il Fornitore si obbliga a: *(a)* dare immediata comunicazione a Consip S.p.A. e alle singole Amministrazioni, di ogni circostanza che abbia influenza sull'esecuzione delle attività di cui all'Accordo Quadro e ai singoli Contratti esecutivi; *(b)* prestare i servizi nei luoghi che verranno indicati nei Contratti esecutivi stessi.
10. Il Fornitore prende atto ed accetta che i servizi oggetto dell'Accordo Quadro dovranno essere prestati con continuità anche in caso di eventuali variazioni della consistenza e della dislocazione delle sedi e degli uffici delle Amministrazioni.
11. Nel rispetto della normativa vigente i servizi oggetto dell'Accordo Quadro e dei singoli Contratti esecutivi non sono affidati al Fornitore in via esclusiva, pertanto le Amministrazioni possono affidare le stesse forniture, attività e servizi anche a soggetti terzi, diversi dal medesimo Fornitore.
12. Il Fornitore è tenuto a comunicare a Consip S.p.A. e alle altre Amministrazione ogni modificazione negli assetti proprietari, nella struttura di impresa e negli organismi tecnici e amministrativi. Tale comunicazione dovrà pervenire a Consip S.p.A. entro 15 (quindici) giorni dall'intervenuta modifica.
13. Ai sensi dell'art. 105, comma 2, D.Lgs. n. 50/2016, con riferimento a tutti i sub–contratti stipulati dal Fornitore per l'esecuzione del contratto, è fatto obbligo al Fornitore stesso di comunicare, a Consip S.p.A. e all'Amministrazione interessata, il nome del sub-contraente, l'importo del contratto, l'oggetto delle attività, delle forniture e dei servizi affidati. Eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto dovranno essere altresì comunicate a Consip S.p.A. e all'Amministrazione interessata.
14. Si precisa che le attività di coordinamento del presente AQ verranno svolte con il supporto dell'Organismo di Coordinamento e Controllo di cui al Capitolato Tecnico parte generale.
15. Ai sensi dell'art. 47 comma 3bis, della L. n. 108/2021, il Fornitore è tenuto a consegnare alla Committente in relazione a ciascuna impresa e/o consorziata che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1, del d.lgs. n. 198/2006:

    - la certificazione di cui all'articolo 17 della legge 12 marzo 1999, n. 68;
    - una relazione relativa all'assolvimento degli obblighi di cui alla medesima legge n. 68/1999 e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di scadenza di presentazione delle offerte. La relazione dovrà essere trasmessa anche alle rappresentanze sindacali aziendali.

    La documentazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della relazione alle rappresentanze sindacali aziendali, dovrà essere consegnata alla Consip, **entro 6 mesi dalla stipula** dell'Accordo Quadro.
    La violazione anche di uno solo di tali obblighi comporta l'applicazione delle penali di cui al successivo articolo "Penali".
16. La relazione di cui al precedente comma 15 sarà pubblicata sul profilo del Committente, nella sezione "Amministrazione trasparente", ai sensi dell'art. 29, comma 1 del Codice e dell'art. 47, comma 9, della L. n. 108/2021. La Committente procederà anche con gli ulteriori adempimenti di cui al citato articolo 47 comma 9, della L. n. 108/2021.

ARTICOLO 8 - OBBLIGAZIONI SPECIFICHE DEL FORNITORE

1. Il Fornitore dell'Accordo Quadro ha l'obbligo di tenere costantemente aggiornata, per tutta la durata del presente Accordo Quadro, la documentazione amministrativa richiesta e presentata a Consip S.p.A. per la stipula del presente Accordo Quadro. In particolare, pena l'applicazione delle penali di cui oltre, ciascun Fornitore ha l'obbligo di:
   a) comunicare, entro 15 (quindici) giorni dall'intervenuta modifica e/o integrazione, ogni modificazione e/o integrazione relativa al possesso dei requisiti di cui al paragrafo III.1.1 del Bando di gara;
   b) comunicare, entro 15 (quindici) giorni dalle intervenute modifiche, le modifiche soggettive di cui all'art. 80 del D.Lgs. n. 50/2016;
   c) comunicare alla Consip S.p.A. ogni modifica o il venir meno dei requisiti attestanti la capacità tecnica richiesta (Certificazioni ISO 9001) ai fini della partecipazione, entro il termine perentorio di 15 (quindici) giorni lavorativi decorrenti dall'evento modificativo.
2. Il Fornitore in adempimento di quanto previsto dall' articolo 22 del Regolamento UE/2021/241 del 12 febbraio 2021, in tema di tutela degli interessi finanziari dell'Unione Europea, ha dichiarato i dati identificativi dei titolari effettivi, anche eventualmente schermati da società fiduciarie

ARTICOLO 9 - VERIFICA DI CONFORMITÀ

1. Con riferimento al singolo Contratto esecutivo, ciascuna Amministrazione Contraente procederà ad effettuare la verifica di conformità dei servizi oggetto di ciascun Contratto esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali; tale verifica, che potrà essere eseguita anche a campione, verrà effettuata, su richiesta di ciascuna Amministrazione secondo le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico Generale e Speciale.
   La verifica di conformità sarà svolta dalle Amministrazioni nel rispetto di quanto stabilito dagli artt. 101 e 102 del D. Lgs. n. 50/2016, nonché di quanto previsto nei provvedimenti di attuazione.
3. Le verifiche di conformità di cui ai precedenti commi si intendono positivamente superate solo se le verifiche abbiano dato esito positivo ed i servizi siano risultati conformi alle prescrizioni dell'Accordo Quadro, del Capitolato Tecnico Generale e Speciale e dell'offerta tecnica, ove migliorativa; tutti gli oneri e le spese delle verifiche di conformità sono a carico del Fornitore.
4. Nel caso di esito positivo della verifica di conformità relativamente ai servizi di compliance e controllo la data del relativo verbale verrà considerata quale "Data di accettazione".
5. Nel caso di esito negativo della verifica di conformità e/o di esito negativo delle verifiche di funzionalità effettuate in corso d'opera a norma del successivo comma, il Fornitore dovrà svolgere ogni attività necessaria affinché la verifica sia ripetuta e positivamente superata, salvo in ogni caso l'applicazione delle penali di cui oltre.
6. Conclusa positivamente la verifica di conformità, e comunque entro un termine non superiore a sette giorni dalla conclusione della stessa, l'Amministrazione Contraente rilascia il certificato di pagamento o altro documento equivalente ai fini dell'emissione della fattura da parte dell'appaltatore.
7. Le Amministrazioni Contraenti e la Consip S.p.A., per quanto di propria competenza, potranno effettuare unilaterali verifiche, anche in corso d'opera, per l'accertamento della conformità dei servizi resi disponibili.
8. Su richiesta del Fornitore, il Responsabile del Procedimento dell'Amministrazione contraente emetterà il certificato di esecuzione prestazioni dei servizi (CES), coerentemente al modello predisposto dall'Autorità Nazionale Anticorruzione. Il certificato verrà emesso solo a seguito della verifica, da parte dell'Amministrazione contraente, dell'avvenuta erogazione dei servizi oggetto del Contratto esecutivo e della conseguente verifica di conformità della fornitura predetta, nel rispetto delle prescrizioni contrattuali e della normativa vigente.

9. In caso di mancata attestazione di regolare esecuzione, la singola Amministrazione potrà risolvere il Contratto esecutivo e provvederà a dare comunicazione a Consip S.p.A. la quale potrà risolvere il presente Accordo Quadro.

ARTICOLO 10 - CORRISPETTIVI E FATTURAZIONE

1. I corrispettivi dovuti al Fornitore dalle singole Amministrazioni Contraenti per le prestazioni oggetto di ciascun Contratto esecutivo sono indicati nell'Offerta Economica, di cui all'Allegato **"B"** del presente Accordo Quadro e nel documento riepilogativo allegato sub **"C"** (Corrispettivi e tariffe PAC).
2. I corrispettivi, indicati nell'Accordo Quadro, si riferiscono ai servizi prestati a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.
3. Tutti gli obblighi ed oneri derivanti al Fornitore dall'esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi, dall'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti Autorità, sono compresi nel corrispettivo contrattuale.
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.
5. Tali corrispettivi sono dovuti dalle Amministrazioni Contraenti al Fornitore a decorrere dalla "Data di accettazione**",** successivamente all'esito positivo della verifica di conformità della prestazione.
6. Ciascuna fattura dovrà contenere, oltre alle indicazioni che verranno fornite dall'Amministrazione, il riferimento all'Accordo Quadro, al singolo Contratto esecutivo, cui si riferisce e dovrà essere intestata e trasmessa alla Amministrazione. Il CIG (Codice Identificativo Gara) "derivato" rispetto a quello dell'Accordo Quadro o il CUP (Codice Unico di Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003, comunicato dalle Amministrazioni sarà inserito, a cura del Fornitore, nelle fatture e dovrà essere indicato dalle Amministrazioni nei rispettivi pagamenti ai fini dell'ottemperanza agli obblighi scaturenti dalla normativa in tema di tracciabilità dei flussi finanziari.
7. Nel caso in cui l'aggiudicatario sia un R.T.I., gli obblighi di cui sopra dovranno essere tutti puntualmente assolti sia nelle fatture emesse dalla mandataria, sia dalle mandanti, nel rispetto delle condizioni e delle modalità tutte disciplinate dai successivi comma del presente articolo.
8. I predetti corrispettivi saranno fatturati con la cadenza indicata in sede di Contratto esecutivo e saranno corrisposti dalle Amministrazioni secondo la normativa vigente in materia di Contabilità delle Amministrazioni Contraenti e previo accertamento della prestazione effettuate.
9. Ciascuna fattura dovrà essere inviata in forma elettronica in osservanza delle modalità previste dal D. Lgs. 20 febbraio 2004 n. 52, dal D. Lgs. 7 marzo 2005 n. 82 e dai successivi decreti attuativi. Il Fornitore si impegna, inoltre, ad inserire nelle fatture elettroniche i dati e le informazioni che la singola Amministrazione Contraente riterrà di richiedere, nei limiti delle disposizioni normative vigenti.
10. Ai fini del pagamento di corrispettivi di importo superiore ad euro 5.000,00, l'Amministrazione Contraente procederà in ottemperanza alle disposizioni previste dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973, con le modalità di cui al Decreto del Ministero dell'Economia e delle Finanze del 18 gennaio 2008 n. 40.
11. Rimane inteso che l'Amministrazione prima di procedere al pagamento del corrispettivo acquisirà di ufficio il documento unico di regolarità contributiva (D.U.R.C.) - attestante la regolarità del Fornitore in ordine al versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti.
12. A decorrere dal 1 Febbraio 2020, per gli acquisti di beni, e dal 1 Gennaio 2021, per gli acquisti di servizi, ai sensi

dell'articolo 1, comma 412, della legge 31 dicembre 2009, n. 196 nonché dall'articolo 3 del Decreto del Ministro dell''Economia e delle Finanze 7 dicembre 2018, così come modificato dal Decreto del Ministero dell'Economia e delle Finanze 27 dicembre 2019, e in conformità alle "Linee Guida per l'emissione della trasmissione degli ordini elettronici adottate dal Ministero dell'Economia e delle Finanze" in data 29 dicembre 2020, l'Amministrazione Contraente rientrante nell'ambito applicativo della normativa sopra richiamata, dovrà, fatta eccezione per le esclusioni previste dal par. 3.1.2 delle richiamate Linee guida, trasmettere al Nodo di Smistamento degli Ordini di acquisto (NSO), il documento informatico attestante l'Ordinativo di Fornitura stesso (di seguito "Ordine NSO"). A tal fine, l'Amministrazione Contraente utilizza la funzione di trasmissione automatica al NSO, disponibile sul Sistema di e-procurement di Consip S.p.A., o, in alternativa, trasmette, l'Ordine NSO attraverso altre piattaforme.

13. Ciascuna fattura relativa agli acquisti, da e per conto degli enti del Servizio sanitario nazionale, di cui all'articolo 19, comma 2, lettere b) e c), del D. Lgs. 23 giugno 2011, n. 118, dovrà riportare gli estremi dei documenti informatici attestanti l'ordinazione e l'esecuzione dell'acquisto, trasmessi per mezzo del NSO. Qualora la fattura non indichi gli estremi dell'Ordine NSO da cui promana, a causa del mancato invio dell'Ordine NSO da parte dell'Ente, quest'ultimo è tenuto a provvedere al mancato invio con la trasmissione di un Ordine di convalida, secondo le modalità indicate nelle Linee Guida sopra richiamate.
14. Le Amministrazioni contraenti opereranno sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5 % che verrà liquidata dalle stesse solo al termine del Contratto esecutivo; le ritenute possono essere svincolare solo in sede di liquidazione finale, in seguito all'approvazione del certificato di verifica di conformità e previa acquisizione del documento unico di regolarità contributiva.
15. I termini di pagamento delle predette fatture saranno definiti secondo le modalità di cui alla normativa vigente, e, in particolare, dell'art. 113 bis del Codice e del D.Lgs. n. 231/2002 s.m.i. I corrispettivi saranno accreditati, a spese dell'Amministrazione Contraente o del Fornitore ove sia previsto da norme di legge o regolamentari, sul conto corrente:
    - n. 000046871576, intestato al Fornitore Intellera Consulting S.r.l. presso Credit Agricole Italia S.p.A., Agenzia 2 di Bologna Via Vittoria, 2/A - 40133 Bologna, Codice IBAN IT32H0623002452000046871576;
    - n. 000042206371, intestato al Fornitore Intellera Consulting S.r.l. presso BPER Banca S.p.A., Via della Moscova, 31a - 20121 Milano, Codice IBAN IT91Z0538701615000042206371;
    - n. 052692540540, intestato al Fornitore Intellera Consulting S.r.l. presso Banca Sella S.p.A., Filiale Via Faruffini, 2 – 20149 Milano, Codice IBAN IT09J0326801600052692540540;
    - n. 010000323475, intestato al Fornitore Intellera Consulting S.r.l. presso Credito Emiliano S.p.A., Agenzia 4 di Milano C.so Sempione, 20 - 20154 Milano, Codice IBAN IT25R0303201603010000323475;
    - n. 100000009429, intestato al Fornitore H.S.P.I. S.p.A. presso Banca Intesa San Paolo, filiale di Bologna Via Farini 22 – 40124 Bologna, Codice IBAN IT62E0306902478100000009429;
    - n. 0002302, intestato al Fornitore Teleconsys S.p.A. presso Banca Nazionale del Lavoro, AG. Roma 83 – 6483 - via Gallia 232 – 00183 Roma, Codice IBAN IT44W0100503306000000002302;
    - n. 000002800175, intestato al Fornitore Capgemini Italia S.p.A. presso Banca Intesa San Paolo, Agenzia 10 – Viale Ciamarra 234 -00173 Roma, Codice IBAN IT 46 K 03069 05058 000002800175;

    Il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e s.m.i.
16. Il Fornitore si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i alle Amministrazioni all'atto dell'accettazione del Piano dei Fabbisogni secondo le modalità indicate all'art.6.
17. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto nell'art. 5 del D.Lgs. 9 ottobre 2002, n. 231.

18. Il Fornitore, sotto la propria esclusiva responsabilità, renderà tempestivamente noto alle Amministrazioni e alla Consip S.p.A., per quanto di propria competenza, le variazioni che si verificassero circa le modalità di accredito indicate nell'Accordo Quadro e nei singoli Contratti esecutivi; in difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, il Fornitore non potrà sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.
19. Nel caso in cui risulti aggiudicatario dell'Accordo Quadro un R.T.I., le singole imprese costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione Contraente, dovranno provvedere ciascuna alla fatturazione delle sole attività effettivamente svolte, corrispondenti alle attività dichiarate in fase di gara risultanti nell'atto costitutivo del Raggruppamento Temporaneo di Imprese, che il Fornitore si impegna a trasmettere in copia, ove espressamente richiesto dall'Amministrazione Contraente. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi e/o forniture cui si riferisce.
20. Il R.T.I. avrà facoltà di scegliere se: i) il pagamento da parte delle Amministrazioni Contraenti dovrà essere effettuato nei confronti della mandataria che provvederà poi alla redistribuzione dei corrispettivi a favore di ciascuna mandante in ragione di quanto di spettanza o ii) se, in alternativa, il pagamento dovrà essere effettuato dalle Amministrazioni Contraenti direttamente a favore di ciascun membro del RTI. La predetta scelta dovrà risultare dall'atto costitutivo del RTI medesimo. In ogni caso, la società mandataria del Raggruppamento medesimo è obbligata a trasmettere apposito prospetto riepilogativo delle attività e delle competenze maturate dalle singole imprese membri del RTI e, in maniera unitaria, le fatture di tutte le imprese raggruppate e prospetto riepilogativo delle attività e delle competenze maturate da ciascuna. Resta in ogni caso fermo quanto previsto dall'art. 48, comma 13, del D.Lgs. n. 50/2016.
21. Resta tuttavia espressamente inteso che in nessun caso il Fornitore potrà sospendere la prestazione dei servizi e, comunque, delle attività previste nell'Accordo Quadro e nei singoli Contratti esecutivi, salvo quanto diversamente previsto nell'Accordo Quadro medesimo.
22. Qualora il Fornitore si rendesse inadempiente a tale obbligo, i singoli Contratti esecutivi e/o l'Accordo Quadro si potranno risolvere di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi tramite pec o con lettera raccomandata A/R, rispettivamente dalle Amministrazioni Contraenti e dalla Consip S.p.A., ciascuno per quanto di propria competenza.
23. E' ammessa la cessione dei crediti maturati dal Fornitore nei confronti dell'Amministrazione a seguito della regolare e corretta esecuzione delle prestazioni oggetto del Contratto esecutivo, nel rispetto dell'art. 106, comma 13, del D.Lgs. n. 50/2016. In ogni caso, è fatta salva ed impregiudicata la possibilità per l'Amministrazione Contraente di opporre al cessionario tutte le medesime eccezioni opponibili al Fornitore cedente. Le cessioni dei crediti devono essere stipulati mediante atto pubblico o scrittura privata autenticata e devono essere notificate alla Amministrazione Contraente. Si applicano le disposizioni di cui alla Legge n. 52/1991. Resta fermo quanto previsto in tema di tracciabilità dei flussi finanziari di cui al successivo articolo 25.
24. Ai fini del versamento dell'IVA per cessione di beni e prestazioni di servizi a favore delle Pubbliche Amministrazioni, si applica quanto previsto dall'art. 17-ter del d.P.R. n. 633 del 1972 ("split payment"), introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96, e le relative disposizioni di attuazione tra le quali il DM 23 gennaio 2015 come modificato dal DM 27 giugno 2017.
25. In caso di pericolo di insolvenza di Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, diversi dalle società pubbliche 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. 196, a totale partecipazione pubblica diretta o indiretta, è facoltà del Fornitore non inadempiente richiedere di

prestare idonea garanzia per l'adempimento dell'obbligazione di pagamento relativa al contratto esecutivo; tale garanzia dovrà essere rilasciata per un importo pari al 20% del valore del Contratto esecutivo. La garanzia dovrà essere richiesta dal Fornitore entro il termine di 4 giorni lavorativi dalla ricezione dell'ordine e l'Amministrazione dovrà rilasciarla entro 30 giorni dalla ricezione della richiesta. Il Fornitore non inadempiente è legittimato a sospendere l'esecuzione della fornitura fino ad avvenuta ricezione della garanzia richiesta. Decorso inutilmente il termine per il rilascio della garanzia e ferma restando la facoltà di sospensione dell'esecuzione, è facoltà del Fornitore, ai sensi dell'art. 1454 c.c., diffidare per iscritto l'Amministrazione ad adempiere entro 15 giorni, decorsi inutilmente i quali il contratto s'intenderà risolto di diritto. Resta salva la facoltà dell'Amministrazione di recedere dal contratto esecutivo in caso di sospensione.

26. In caso di Contratti esecutivi effettuati da Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, verso i quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato del presente AQ o in precedenti rapporti contrattuali, il Fornitore è legittimato a sospendere l'esecuzione del Contratto esecutivo fino ad avvenuta ricezione della comprova del pagamento per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dei suddetti soggetti di recedere dal contratto esecutivo in caso di sospensione.
27. Fermo restando quanto stabilito al precedente comma, in caso di Contratti esecutivi effettuati da Amministrazioni verso le quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato nel presente Accordo Quadro ovvero in precedenti rapporti contrattuali relativi alla fornitura di beni o servizi ricompresi nell'oggetto dell'Accordo Quadro, il Fornitore è legittimato a sospendere l'esecuzione del contratto esecutivo fino ad avvenuta ricezione della comprova del pagamento/stanziamento di fondi per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione all'Amministrazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dell'Amministrazione di recedere dal contratto esecutivo in caso di sospensione.
28. Gli Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, nel Contratto esecutivo, accettano preventivamente la cessione dei crediti ai sensi e per gli effetti di cui all'art. 106, comma 13 del D.Lgs. n. 50/2016.
29. Ove applicabile in considerazione della natura e 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 delle prestazioni oggetto del Contratto esecutivo un'anticipazione del prezzo pari al 20 per cento del valore del Contratto esecutivo stesso. Tale percentuale può essere aumentata dall'Amministrazione Contraente fino ad un massimo del 30% al ricorrere dei presupposti di cui all'art. 207 del D.L. 34/2020.
    L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore dell'Amministrazione 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 sarà indicato nel Piano dei Fabbisogni .
30. L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento delle prestazioni, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.
31. Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione delle prestazioni, 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 della anticipazione.

32. Laddove in relazione al singolo contratto esecutivo ricorrano i presupposti soggettivi ed oggettivi, le Amministrazioni Contraenti e il Fornitore sono tenuti all'applicazione delle disposizioni di cui all'art. 17-bis del D.lgs. 241/1997 in materia di ritenute e compensazioni in appalti e subappalti.

ARTICOLO 11 - COSTI DELLA SICUREZZA

1. Stante la natura delle prestazioni oggetto di Accordo Quadro non è prevista la redazione del "Documento di valutazione dei rischi standard da interferenze".

ARTICOLO 12 - PENALI

1. Si applicano le penali previste nell'appendice 1 al Capitolato Tecnico Speciale (che deve intendersi in questa sede integralmente trascritta), nonché quelle di seguito indicate. È sempre fatto salvo il risarcimento del maggior danno. In caso di penali da ritardo, deve considerarsi ritardo anche il caso in cui il Fornitore esegua il servizio in modo anche solo parzialmente difforme rispetto alle disposizioni di cui al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto esecutivo, nonché alla propria Offerta Tecnica. In tal caso le Amministrazioni applicheranno al Fornitore la suddetta penale sino alla data in cui il servizio inizierà ad essere eseguito in modo effettivamente conforme al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto esecutivo, all'Offerta Tecnica, fatto salvo il risarcimento del maggior danno.
2. In caso di invio della documentazione necessaria all'attivazione dell'Accordo Quadro (ivi compreso il Piano di Qualità Generale) in ritardo rispetto ai termini previsti nel presente Accordo Quadro e relativi allegati o di ritardo nell'attivazione del portale della fornitura, per cause non imputabili a Consip ovvero a forza maggiore o caso fortuito, Consip avrà la facoltà di applicare una penale pari a 1.000,00 euro per ogni giorno solare di ritardo, fatto salvo il risarcimento del maggior danno subito.
3. In caso di invio della documentazione prodromica alla stipula di ciascun Contratto Esecutivo (ivi compreso il Piano Operativo e relativi allegati e i riferimenti del RUAC del Contratto Esecutivo) in ritardo rispetto ai termini previsti nel presente Accordo Quadro e relativi allegati o comunque concordati con l'Amministrazione, per cause non imputabili a Consip, all'Amministrazione ovvero a forza maggiore o caso fortuito, Consip, anche su segnalazione dell'Amministrazione, avrà la facoltà di applicare una penale pari a 1.000,00 euro per ogni giorno solare di ritardo, fatto salvo il risarcimento del maggior danno subito.
4. Per ogni giorno di ritardo del Fornitore, non imputabile a Consip S.p.A. ovvero a forza maggiore o caso fortuito, nell'adempimento all'obbligo previsto al precedente articolo 8, comma 1, lettere a), b) e c) per la presentazione della documentazione ivi indicata, il Fornitore è tenuto a corrispondere a Consip S.p.A. una penale pari a euro 100,00 = (cento/00), fatto salvo il risarcimento del maggior danno.
5. Per ogni giorno di ritardo non imputabile all'Amministrazione, ovvero a forza maggiore o caso fortuito, i) rispetto ai previsti tempi di effettuazione delle verifiche di conformità; ii) di ripetizione delle prove di collaudo in caso di esito negativo delle verifiche di conformità; l'Amministrazione potrà applicare al Fornitore una penale pari allo 0,3 (ovvero in caso di Contratti esecutivi cd. PNRR o PNC si intenderà 0,6) per mille del valore del Contratto esecutivo, fatto salvo il risarcimento del maggior danno.
6. Nel caso in cui, come previsto nell'atto di nomina a responsabile del Trattamento allegato all'Accordo Quadro, all'esito delle verifiche, ispezioni e audit e assessment compiuti dall'Amministrazione o da terzi autorizzati, le misure di sicurezza adottate dal Responsabile primario/Sub responsabile/terzo autorizzato al trattamento dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione delle "*Norme in materia di protezione dei*

dati personali", l'Amministrazione applicherà al Fornitore - Responsabile primario/Sub responsabile/terzo autorizzato al trattamento una penale pari all' **1 per mille** del corrispettivo del singolo Contratto esecutivo per ogni giorno necessario per il Fornitore per l'adozione di misure di sicurezza idonee ad assicurare l'applicazione delle "*Norme in materia di protezione dei dati personali*", salvo il maggior danno.

7. Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali sopra stabilite, dovranno essere contestati al Fornitore per iscritto da Consip S.p.A. e/o dalla singola Amministrazione, per quanto di rispettiva competenza; in quest'ultimo caso, gli eventuali inadempimenti dovranno essere comunicati dalle Amministrazioni per conoscenza a Consip S.p.A.
8. In caso di mancato adempimento anche ad una sola delle obbligazioni di cui al precedente art. 7, comma 15 il Fornitore sarà tenuto a corrispondere, ai sensi dell'art. 47, comma 6 della L. n. 108/2021 una penale pari a euro 25.000,00. Il mancato adempimento dell'invio della documentazione richiesta entro 30 giorni dall'applicazione della penale comporta l'applicazione di una ulteriore penale del medesimo importo fino ad avvenuto adempimento e comunque, a parziale deroga di quanto previsto dal successivo comma 13, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro.
9. Per ogni punto percentuale di scostamento in diminuzione (arrotondato al numero intero) tra il valore percentuale misurato e il valore minimo richiesto al par. 7.1 del Capitolato Tecnico Generale (**dati per Consip**) Consip, si riserva di applicare una penale pari a euro 1.000,00.
10. Per ogni punto percentuale di scostamento in diminuzione (arrotondato al numero intero) tra il valore percentuale minimo richiesto al par. 7.1 del Capitolato Tecnico Generale (**dati per Amministrazione**) e il valore percentuale come eventualmente migliorato nella propria offerta tecnica dal Fornitore l'Amministrazione, si riserva di applicare una penale pari a euro 1.000,00.
11. In caso di contestazione dell'inadempimento da parte di Consip S.p.A. e/o della singola Amministrazione, per quanto di rispettiva competenza, il Fornitore dovrà comunicare, in ogni caso, per iscritto, le proprie deduzioni, supportate da una chiara ed esauriente documentazione, nel termine massimo di n. 5 (cinque) giorni lavorativi dalla ricezione della contestazione stessa. Qualora le predette deduzioni non pervengano a Consip S.p.A. e/o all'Amministrazione nel termine indicato, ovvero, pur essendo pervenute tempestivamente, non siano idonee, a giudizio di Consip S.p.A. e/o dall'Amministrazione, a giustificare l'inadempienza, potranno essere applicate al Fornitore le penali stabilite nell'Accordo Quadro a decorrere dall'inizio dell'inadempimento.
12. Consip S.p.A. potrà per l'applicazione delle penali dell'Accordo Quadro avvalersi della garanzia disciplinata nell'Accordo Quadro, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario. Le singole Amministrazioni potranno compensare i crediti derivanti dall'applicazione delle penali di cui all'Accordo Quadro con quanto dovuto al Fornitore a qualsiasi titolo, quindi anche con i corrispettivi maturati, ovvero avvalersi della garanzia disciplinata nell'Accordo Quadro, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario.
13. Consip S.p.A., per le parti di sua competenza, potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) del valore dell'Accordo Quadro, fermo il risarcimento degli eventuali maggiori danni, nonché la risoluzione contrattuale per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima.
14. Le Amministrazioni, per le parti di loro competenza, potranno applicare al Fornitore penali sino a concorrenza della misura massima:
    - pari al 20% (venti per cento), per i contratti finanziati in tutto o in parte con i fondi del PNRR e del PNC,
    - ovvero
    - pari al 10% (dieci per cento), per i contratti non finanziati con i fondi del PNRR o del PNC;

    del Contratto di Fornitura, fermo il risarcimento degli eventuali maggiori danni, nonché la risoluzione contrattuale

per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima

15. La richiesta e/o il pagamento delle penali non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

ARTICOLO 13 - GARANZIE

1. A garanzia delle obbligazioni contrattuali assunte nei confronti della Consip S.p.A. dal Fornitore con la stipula della Accordo Quadro, il Fornitore medesimo ha prestato garanzia definitiva rilasciata in data 04/02/2022 dalla Coface avente n. 2343646 di importo pari ad Euro 100.000,00 = (centomila/00).
2. In particolare, la garanzia rilasciata garantisce tutti gli obblighi specifici assunti dal Fornitore, anche quelli a fronte dei quali è prevista l'applicazione di penali da parte di Consip e quelli derivanti dal rispetto del patto di integrità, pertanto, resta espressamente inteso che la stessa Consip, fermo restando quanto previsto nel precedente articolo 12, ha diritto di rivalersi direttamente sulla garanzia per l'applicazione delle penali. Tale garanzia copre altresì la serietà dell'offerta dell'aggiudicatario nell'ambito della fase di affidamento dei singoli Contratti esecutivi prevista dal paragrafo 6.5 del Capitolato Tecnico Generale e dall'art. 6 del presente documento, ivi compresa la fase di rilascio del Piano Operativo. La stessa garanzia verrà, altresì, escussa nel caso di dichiarazioni mendaci rese nell'ambito dell'aggiornamento della documentazione amministrativa di cui all'art. 8 dell'Accordo Quadro. In tal caso la Consip procederà, oltre alla risoluzione dell'Accordo Quadro, anche alla segnalazione del fatto all'Autorità Nazionale Anticorruzione.
3. La garanzia prestata in favore della Consip S.p.A. opera a far data dalla sottoscrizione dell'Accordo Quadro e per tutta la durata dell'Accordo Quadro e dei Contratti esecutivi, e, comunque, sino alla completa ed esatta esecuzione delle obbligazioni nascenti dai predetti contratti.
4. A garanzia delle obbligazioni contrattuali assunte dal Fornitore con la stipula dell'Accordo Quadro e dei relativi Contratti esecutivi, il Fornitore medesimo si è impegnato a prestare in favore di ciascuna Amministrazione Contraente la relativa garanzia definitiva in conformità al modello 2 di cui all'Allegato 14 della documentazione di gara.
5. La garanzia copre tutti gli obblighi specifici assunti dal Fornitore con i contratti esecutivi nei confronti delle Amministrazioni, anche quelli a fronte dei quali è prevista l'applicazione di penali da parte delle stesse e, pertanto, resta espressamente inteso che le Amministrazioni hanno diritto di rivalersi direttamente sulla garanzia per l'applicazione delle penali. La garanzia copre altresì il risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, 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 il rispetto degli impegni assunti con il Patto di integrità, l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione dei contratti esecutivi disposta in danno dell'esecutore, il pagamento di quanto dovuto dall'esecutore 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.
6. La garanzia prestata in favore delle Amministrazioni decorre dalla data di stipula di ciascun contratto esecutivo e cessa alla data di emissione del certificato di verifica di conformità o dell'attestazione di regolare esecuzione delle prestazioni, emessi alla conclusione dell'esecuzione del medesimo contratto e comunque decorsi 12 mesi dalla data di ultimazione delle prestazioni contrattuali risultante dal relativo certificato dell'ultimo contratto esecutivo, allorché si estingue automaticamente ad ogni effetto (art. 103, commi 1 e 5, del Codice). Resta fermo quanto previsto nello schema tipo del DM 31/2018 come derogato dal Capitolato d'Oneri.
7. Le garanzie di cui ai precedenti commi prevedono espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, comma 2, del codice civile,

nonché l'operatività della garanzia medesima – anche per il recupero delle penali contrattuali - entro quindici giorni, a semplice richiesta scritta del rispettivo beneficiario.

8. E' onere della singola Amministrazione comunicare alla Consip S.p.a. l'importo delle somme percepite dal Garante.
9. Le garanzie di cui ai commi precedenti sono progressivamente svincolate in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80 per cento dell'iniziale importo garantito secondo quanto stabilito all'art. 103, comma 5, del D.Lgs. n. 50/2016. Lo svincolo avviene subordinatamente alla preventiva consegna al Garante ed alla Consip S.p.A da parte del Fornitore, in relazione ai contratti stipulati nell'arco temporale di riferimento, di: *(i)* documenti delle Amministrazioni, in originale o in copia autentica, attestanti la corretta esecuzione delle prestazioni, ai sensi dell'articolo 102 del D.Lgs. n. 50/2016; e/o *(ii)* documentazione comprovante l'avvenuta ricezione del rimborso della ritenuta di legge dello 0,5%, di cui al precedente articolo 10, comma 14. Il Garante dovrà comunicare alla Consip il valore dello svincolo. La Consip S.p.a. si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.
10. In alternativa a quanto sopra, il Fornitore potrà consegnare alla Consip S.p.a. un prospetto contenente l'elenco delle Amministrazioni Contraenti con l'ammontare delle fatture emesse nel relativo arco temporale e regolarmente saldate, unitamente al dettaglio specifico della posizione di ciascuna singola Amministrazione Contraente (numero fattura, numero contratto, mensilità di riferimento, data emissione, data pagamento, importo corrisposto), accompagnato da dichiarazione resa dal legale rappresentante del Fornitore o procuratore speciale munito dei necessari poteri, ai sensi del D.P.R. n. 445/2000, attestante la veridicità di tutte le informazioni contenute nel prospetto stesso e l'assenza di ogni contestazione sulle prestazioni eseguite e in esso consuntivate. La Consip S.p.a. procederà ad autorizzare lo svincolo comunicandolo al Garante e al Fornitore.
11. Ai fini dello svincolo dell'ammontare residuo delle garanzie (20%), il Fornitore dovrà produrre, in relazione ai rimanenti Contratti esecutivi: *(i)* i certificati di verifica di conformità o le attestazioni di regolare esecuzione delle prestazioni emessi alla conclusione dell'esecuzione dei contratti esecutivi; e/o *(ii)* documentazione comprovante il rimborso della ritenuta di legge dello 0,5%, di cui al precedente articolo 10, comma 14.
12. Qualora l'ammontare delle garanzie prestate dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, il Fornitore dovrà provvedere al reintegro entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta effettuata dalla Consip S.p.A., pena la risoluzione della Accordo Quadro e/o dei singoli contratti esecutivi.
13. In caso di inadempimento alle obbligazioni previste nel presente articolo la Consip S.p.A. ha facoltà di dichiarare risolto l'Accordo Quadro e, del pari, le singole Amministrazioni Contraenti hanno facoltà di dichiarare risolto il contratto esecutivo, fermo restando il risarcimento del danno.
14. In ogni caso il garante sarà liberato dalle garanzie prestate di cui ai commi precedenti solo previo consenso espresso in forma scritta dalla Consip S.p.A..

ARTICOLO 14 - RISOLUZIONE

1. Consip e/o le Amministrazioni, per quanto di rispettiva competenza, senza bisogno di assegnare alcun termine per l'adempimento, potranno risolvere l'Accordo Quadro e il singolo Contratto esecutivo ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art.1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
   a) il Fornitore si è trovato, al momento dell'aggiudicazione dell'Accordo Quadro in una delle situazioni di cui

all'articolo 80, comma 1, del d. lgs. n. 50/2016 e s.m.i. e avrebbe dovuto pertanto essere escluso dalla gara;

b) il Fornitore ha commesso, nella procedura di aggiudicazione del presente Accordo Quadro e/o dei successivi Contratti esecutivi, un illecito antitrust accertato con provvedimento esecutivo dell'AGCM, ai sensi dell'articolo 80, comma 5, lett. c) del d. lgs. n. 50/2016 e s.m.i. e secondo le linee guida A.N.AC.;
c) l'Accordo Quadro non avrebbe dovuto essere aggiudicato al Fornitore in considerazione di una grave violazione degli obblighi derivanti dai Trattati, come riconosciuto dalla Corte di giustizia dell'Unione europea in un procedimento ai sensi dell'articolo 258 TFUE;
d) qualora fosse accertata la non sussistenza ovvero il venir meno di uno dei requisiti minimi richiesti per la partecipazione alla gara, nonché per la stipula dell'Accordo Quadro e per lo svolgimento delle attività ivi previste;
e) qualora il Fornitore ponga in essere comportamenti tesi a eludere la modalità di affidamento dei Contratti esecutivi;
f) mancata copertura dei rischi durante tutta la vigenza dell'Accordo Quadro e dei Contratti esecutivi;
g) qualora il Fornitore, in esecuzione di un Contratto esecutivo, offra o fornisca la prestazione di servizi, che non abbiano i requisiti di conformità e/o le caratteristiche tecniche minime stabilite dalle normative vigenti, nonché nel Capitolato Tecnico Generale e Speciale, ovvero quelle migliorative eventualmente offerte in sede di aggiudicazione dell'Accordo Quadro;
h) mancata reintegrazione della garanzia di cui all'art. 13 eventualmente escussa entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta da parte della Consip S.p.A.;
i) azioni giudiziarie per violazioni di diritti di brevetto, di autore ed in genere di privativa altrui, intentate contro le Amministrazioni e/o la Consip S.p.A., ai sensi dell'articolo 21;
j) nei casi di cui agli articoli 9 (Verifiche di conformità); 10 (Corrispettivi e Fatturazione), 17 (Trasparenza), 18 (Riservatezza), 20 (Divieto di cessione del contratto), 24 (Codice Etico - Modello di organizzazione e gestione ex D.Lgs. n. 231/2001 - Piano Triennale per la prevenzione della corruzione e della trasparenza) e 25 (Tracciabilità dei flussi finanziari), 26 (Subappalto), 27 (Danni, responsabilità civile);
k) applicazione di penali oltre la misura massima stabilita all'articolo 12, commi 10 e 11;
l) nell'ipotesi di non veridicità delle dichiarazioni rese dal Fornitore ai sensi del D.p.r. n. 445/00, fatto salvo quanto previsto dall'art. 71, del medesimo D.P.R. 445/2000;
m) nell'ipotesi di irrogazione di sanzioni interdittive o misure cautelari di cui al D. Lgs. n. 231/01, che impediscano all'Impresa di contrattare con le Pubbliche Amministrazioni;
n) in caso di avvalimento, ove a fronte delle segnalazioni delle Amministrazioni contraenti ed in ragione di quanto dichiarato dal Fornitore, risultasse la violazione dell'art. 89, comma 9, del d. lgs. n. 50/2016 e s.m.i.;
o) nei casi di cui all'articolo 3 e 5 del Patto di integrità.

Nelle fattispecie di cui al presente comma non si applicano i termini previsti dall'articolo 21-nonies della legge 7 agosto 1990 n. 241.

2. Consip e/o le Amministrazioni Contraenti, per quanto di rispettiva competenza, devono risolvere l'Accordo Quadro e il singolo Contratto esecutivo senza bisogno di assegnare alcun termine per l'adempimento, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art.1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
   a) qualora nei confronti del Fornitore sia intervenuto un provvedimento definitivo che dispone l'applicazione di una o più misure di prevenzione di cui al codice delle leggi antimafia e delle relative misure di prevenzione, fatto salvo quanto previsto dall'art. 95 del D. Lgs. n. 159/2011, o nel caso in cui gli accertamenti antimafia presso la Prefettura competente risultino positivi oppure sia intervenuta sentenza di condanna

passata in giudicato per i reati di cui all'articolo 80 del D. Lgs. n. 50/2016 e s.m.i.;

b) qualora fosse accertato il venir meno dei requisiti richiesti dalla legge;

3. Inoltre, Consip S.p.a. si impegna ad avvalersi della clausola risolutiva espressa di cui all'art. 1456 c.c. ogni qualvolta nei confronti del Fornitore o dei componenti la propria compagine sociale, o dei dirigenti dell'impresa con funzioni specifiche relative all'affidamento alla stipula e all'esecuzione dell'Accordo Quadro sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317 cp 318 cp 319 cp 319 bis cp 319 ter cp 319 quater 320 cp 322 cp 322 bis cp 346 bis cp 353 cp 353 bis cp. La risoluzione di cui al periodo precedente è subordinata alla preventiva comunicazione all'ANAC, cui spetta la valutazione in merito all'eventuale prosecuzione del rapporto contrattuale, al ricorrere delle condizioni di cui all'art. 32 del dl. 90/2014 convertito in legge 114 del 2014.
4. Il Fornitore accetta le cause di risoluzione previste nell'atto di nomina a Responsabile/sub Responsabile del Trattamento allegato al presente Accordo quadro, che devono intendersi integralmente trascritte.
5. Consip e/o le Amministrazioni Contraenti, quando accertino un grave inadempimento del Fornitore ad una delle obbligazioni assunte con l'Accordo Quadro e/o con i Contratti esecutivi tale da compromettere la buona riuscita delle prestazioni, formuleranno la contestazione degli addebiti al Fornitore e contestualmente assegneranno un termine, non inferiore a quindici giorni, entro i quali il Fornitore dovrà presentare le proprie controdeduzioni. Acquisite e valutate negativamente le controdeduzioni ovvero scaduto il termine senza che il Fornitore abbia risposto, Consip e/o le Amministrazioni Contraenti hanno la facoltà, per quanto di rispettiva competenza, di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei Contratti esecutivi, di incamerare la garanzia ove essa non sia stata ancora restituita ovvero di applicare una penale equivalente, nonché di procedere all'esecuzione in danno dell'Impresa; resta salvo il diritto al risarcimento dell'eventuale maggior danno.
6. Qualora il Fornitore ritardi per negligenza l'esecuzione delle prestazioni rispetto alle previsioni dell'Accordo Quadro e dei Contratti esecutivi, Consip e/o le Amministrazioni contraenti assegnano un termine che, salvo i casi d'urgenza, non può essere inferiore a 10 (dieci) giorni, entro i quali il Fornitore deve eseguire le prestazioni. Scaduto il termine assegnato, e redatto processo verbale in contraddittorio con il Fornitore, qualora l'inadempimento permanga, Consip e/o le Amministrazioni contraenti potranno risolvere l'Accordo Quadro e/o i Contratti esecutivi, fermo restando il pagamento delle penali.
7. In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con la stipula dell'Accordo Quadro e dei Contratti esecutivi che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato tramite pec dalla Consip e/o dall'Amministrazione Contraente, per quanto di propria competenza, per porre fine all'inadempimento, la Consip e/o l'Amministrazione Contraente hanno la facoltà di considerare risolti di diritto l'Accordo Quadro e/o i Contratti esecutivi e di ritenere definitivamente la garanzia ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.
8. In caso di risoluzione anche di uno solo dei Contratti esecutivi, Consip S.p.A. si riserva di risolvere il presente Accordo Quadro. La risoluzione dell'Accordo Quadro legittima la risoluzione dei singoli Contratti esecutivi a partire dalla data in cui si verifica la risoluzione dell'Accordo Quadro. La risoluzione dell'Accordo Quadro è, pertanto, causa ostativa all'affidamento di nuovi Contratti esecutivi e può essere causa di risoluzione dei singoli Contratti esecutivi, salvo che non sia diversamente stabilito nei medesimi e salvo, in ogni caso, il risarcimento del danno.
9. In tutti i casi di risoluzione dell'Accordo Quadro e dei Contratti esecutivi, Consip S.p.A. e/o l'Amministrazione Contraente, avranno diritto di escutere la garanzia prestata per l'intero importo della stessa o per la parte

percentualmente proporzionale all'importo del/i Contratto/i esecutivo/i risolto/i. Ove l'escussione non sia possibile sarà applicata una penale di equivalente importo, che sarà comunicata al Fornitore via pec. In ogni caso, resta fermo il diritto della medesima Amministrazione Contraente e/o di Consip S.p.A. al risarcimento dell'ulteriore maggior danno.

10. La Consip S.p.A., fermo restando quanto previsto nel presente articolo e nei casi di cui all'art. 110 del D.Lgs. n. 50/2016, potrà interpellare progressivamente gli operatori economici che hanno partecipato all'originaria procedura di gara e risultanti dalla relativa graduatoria al fine di stipulare un nuovo Accordo Quadro per l'affidamento del completamento delle prestazioni contrattuali alle medesime condizioni già proposte dall'aggiudicatario in sede di offerta.

ARTICOLO 15 - RECESSO

1. La Consip S.p.A. e/o le Amministrazioni, per quanto di proprio interesse, hanno diritto di recedere unilateralmente dal presente Accordo Quadro e/o da ciascun singolo Contratto esecutivo, in tutto o in parte, in qualsiasi momento, senza preavviso, nei casi di:
   a) giusta causa,
   b) reiterati inadempimenti del Fornitore, anche se non gravi.

   Si conviene che per giusta causa si intende, a titolo meramente esemplificativo e non esaustivo:
   - qualora sia stato depositato contro il Fornitore un ricorso ai sensi della legge fallimentare o di altra legge applicabile in materia di procedure concorsuali, che proponga lo scioglimento, la liquidazione, la composizione amichevole, la ristrutturazione dell'indebitamento o il concordato con i creditori, ovvero nel caso in cui venga designato un liquidatore, curatore, custode o soggetto avente simili funzioni, il quale entri in possesso dei beni o venga incaricato della gestione degli affari del Fornitore, resta salvo quanto previsto dall'art. 110, comma 3, del D.Lgs. n. 50/2016;
   - in qualsiasi altra fattispecie che faccia venire meno il rapporto di fiducia sottostante il presente Accordo Quadro o i Contratti esecutivi.
2. In caso di mutamenti di carattere organizzativo interessanti l'Amministrazione che abbiano incidenza sull'esecuzione della fornitura o della prestazione dei servizi, la stessa Amministrazione potrà recedere in tutto o in parte unilateralmente da Contratto esecutivo, con un preavviso almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore tramite pec.
3. Fermo restando quanto previsto dagli artt. 88, comma 4-ter, e 92, comma 4, del D.Lgs. 159/2011, Consip S.p.A. e/o l'Amministrazione ai sensi dell'art. 109 comma 1 del Codice potrà recedere dall'Accordo Quadro e/o da ciascun singolo contratto esecutivo, in qualunque momento, con preavviso non inferiore a 20 (venti) giorni solari, previo il pagamento da parte delle Amministrazioni delle prestazioni oggetto di Contratto esecutivo eseguite a regola d'arte, nonché del valore dei materiali utili esistenti in magazzino (ove esistenti), oltre al decimo dell'importo delle opere, dei servizi o delle forniture non eseguite, ai sensi dell'art. 109 comma 2 del Codice, rinunciando espressamente il Fornitore, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso e/o indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ..
4. Qualora la Consip receda dall'Accordo Quadro, non potranno essere affidati nuovi Contratti esecutivi da parte delle Amministrazioni e le singole Amministrazioni potranno a loro volta recedere dai singoli Contratti esecutivi, con un preavviso di almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore tramite pec..

ARTICOLO 16 - OBBLIGHI DERIVANTI DAL RAPPORTO DI LAVORO

1. Il Fornitore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative

e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, in materia previdenziale e infortunistica, assumendo a proprio carico tutti i relativi oneri. In particolare, il Fornitore si impegna a rispettare nell'esecuzione delle obbligazioni derivanti dall'Accordo Quadro e dai singoli Contratti esecutivi le disposizioni di cui al D.Lgs. 9 aprile 2008 n. 81.

2. Il Fornitore si obbliga altresì ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, le condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi ed integrativi di lavoro applicabili alla data di stipula dell'Accordo Quadro alla categoria e nelle località di svolgimento delle attività, nonché le condizioni risultanti da successive modifiche ed integrazioni, anche tenuto conto di quanto previsto all'art. 95, comma 10 e all'art. 97 del D. Lgs. n. 50/2016.
3. Il Fornitore si obbliga, altresì, fatto in ogni caso salvo il trattamento di miglior favore per il dipendente, a continuare ad applicare i suindicati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione.
4. Gli obblighi relativi ai contratti collettivi nazionali di lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui questi non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità dell'Accordo Quadro e dei singoli Contratti esecutivi.
5. Restano fermi gli oneri e le responsabilità in capo al Fornitore di cui all'art. 105, comma 9, del D. Lgs. n. 50/2016 in caso di subappalto.

ARTICOLO 17 - TRASPARENZA

1. Il Fornitore espressamente ed irrevocabilmente:
   a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione dell'Accordo Quadro;
   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 dell'Accordo Quadro 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 dell'Accordo Quadro rispetto agli obblighi con esso assunti, né a compiere azioni comunque volte agli stessi fini;
   d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.lgs. 50/2016 al fine di evitare situazioni di conflitto d'interesse.
2. Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse per tutta la durata dell'Accordo Quadro gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma, lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'articolo 1456 cod. civ., per fatto e colpa del Fornitore, con facoltà di Consip S.p.A. di incamerare la garanzia prestata.
3. Il Fornitore si impegna al rispetto di tutte le previsioni di cui al Patto di integrità.

ARTICOLO 18 - RISERVATEZZA

1. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi compresi quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione dell'Accordo Quadro e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
2. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione dell'Accordo Quadro e degli Contratti esecutivi; tale obbligo non concerne i dati che siano o divengano di pubblico dominio.

3. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza anzidetti.
4. In caso di inosservanza degli obblighi di riservatezza, le Amministrazioni e/o Consip S.p.A. hanno la facoltà di dichiarare risolto di diritto, rispettivamente, il singolo Contratto esecutivo ovvero l'Accordo Quadro, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare alle Amministrazioni e/o a Consip S.p.A..
5. Il Fornitore potrà citare i contenuti essenziali dell'Accordo Quadro e dei Contratti esecutivi affidati in proprio favore nei casi in cui ciò fosse condizione necessaria per la partecipazione del Fornitore medesimo a gare e appalti.
6. Resta fermo quanto previsto nel successivo articolo 23.

ARTICOLO 19 - RESPONSABILE UNICO DELLE ATTIVITA CONTRATTUALI (RUAC)

1. Il Responsabile Unico delle Attività Contrattuali (RUAC), nominato dal Fornitore è il Dott. Claudio Paganelli.
2. Il RUAC è il referente responsabile nei confronti di Consip S.p.A. e/o delle Amministrazioni per l'esecuzione del presente Accordo Quadro e dei singoli Contratti esecutivi, e quindi, avrà la capacità di rappresentare ad ogni effetto il Fornitore, salvo quant'altro previsto nel Capitolato Tecnico Generale e Speciale.
3. Qualora il Fornitore dovesse trovarsi nella necessità di sostituire il RUAC, dovrà darne immediata comunicazione scritta a Consip S.p.A.

ARTICOLO 20 - DIVIETO DI CESSIONE DEL CONTRATTO

1. E' fatto assoluto divieto a ciascun Fornitore di cedere, a qualsiasi titolo, l'Accordo Quadro ed i Contratti esecutivi, a pena di nullità della cessione medesima, fatto salvo quanto previsto dall'art. 106, comma 1, lett. d), del d. lgs. n. 50/2016 e s.m.i..
2. In caso di inadempimento da parte del Fornitore degli obblighi di cui al presente articolo, Consip S.p.A. e le Amministrazioni, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolto di diritto l'Accordo Quadro e i Contratti esecutivi.

ARTICOLO 21 - BREVETTI INDUSTRIALI E DIRITTI D'AUTORE

1. Il Fornitore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui; il Fornitore, pertanto, si obbliga a manlevare l'Amministrazione e la Consip S.p.A., per quanto di propria competenza, dalle pretese che terzi dovessero avanzare in relazione a diritti di privativa vantati da terzi.
2. Qualora venga promossa nei confronti delle Amministrazioni e/o di Consip S.p.A. azione giudiziaria da parte di terzi che vantino diritti sulle prestazioni contrattuali, il Fornitore assume a proprio carico tutti gli oneri conseguenti, incluse le spese eventualmente sostenute per la difesa in giudizio. In questa ipotesi, l'Amministrazione e/o Consip S.p.A. sono tenute ad informare prontamente per iscritto il Fornitore in ordine alle suddette iniziative giudiziarie.
3. Nell'ipotesi di azione giudiziaria per le violazioni di cui al comma precedente tentata nei confronti di Consip S.p.A. e delle Amministrazioni e/o, le prime, fermo restando il diritto al risarcimento del danno nel caso in cui la pretesa azionata sia fondata, hanno facoltà di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei singoli Contratti esecutivi, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per i servizi e/o le forniture erogati.

ARTICOLO 22 - FORO COMPETENTE

Per tutte le questioni relative ai rapporti tra il Fornitore e Consip S.p.A. inerenti il presente Accordo Quadro, sarà

competente in via esclusiva il Foro di Roma.

ARTICOLO 23 - TRATTAMENTO DEI DATI PERSONALI

1. Il Fornitore dichiara di aver ricevuto prima della sottoscrizione del presente Accordo Quadro le informazioni di cui all'articolo 13 del "Regolamento UE", circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione dell'Accordo Quadro stesso e dei Contatti derivanti dagli Contratti esecutivi e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa. Tale informativa è contenuta nell'ambito del Capitolato d'Oneri al paragrafo 26 che deve intendersi in quest'ambito integralmente trascritto.
2. Con la sottoscrizione dell'Accordo Quadro, il rappresentante legale del Fornitore acconsente espressamente al trattamento dei dati personali come sopra definito e si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione dell'Accordo Quadro e dei Contatti attuativi, per le finalità descritte nell'informativa resa nel Capitolato d'oneri come sopra richiamata.
3. Le Amministrazioni Contraenti e qualsivoglia altro soggetto pubblico o privato aderendo all'Accordo Quadro, acconsentono espressamente al trattamento ed all'invio a Consip S.p.A. da parte del Fornitore e/o delle singole Amministrazioni, dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione dell'Accordo Quadro e Contratti esecutivi.
4. In adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 1, comma 16, lett. b, e comma 32 L. 190/2012; art. 35 D. Lgs. n. 33/2013; nonché art. 29 D. Lgs. n. 50/2016), il concorrente/contraente prende atto ed acconsente a che i dati e la documentazione che la legge impone di pubblicare, siano pubblicati e diffusi, ricorrendone le condizioni, tramite il sito internet **www.consip.it**, sezione "Società Trasparente"; inoltre, il nominativo del concorrente aggiudicatario della gara ed il prezzo di aggiudicazione dell'appalto, saranno diffusi tramite i siti internet **www.acquistinretepa.it** e **www.mef.gov.it**.
5. Con la sottoscrizione dell'Accordo Quadro ed il perfezionamento dei Contratti esecutivi, il Fornitore acconsente espressamente al trattamento dei dati personali e si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente (Regolamento UE 2016/679 D. Lgs. n. 196/2003 e s.m.i. e D. Lgs. n. 101/2018), ivi inclusi gli ulteriori provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la Protezione dei Dati Personali. In particolare, il Fornitore si impegna ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti.
6. Ove applicabile, in ragione dell'oggetto dell'Accordo Quadro, ove il Fornitore sia chiamato ad eseguire attività di trattamento di dati personali, il medesimo potrà essere nominato "Responsabile/sub-Responsabile del trattamento" dei dati personali ai sensi dell'art. 28 del Regolamento UE sulla base dell'atto di nomina allegato al presente Accordo Quadro. In tal caso, il Fornitore si impegna ad accettare la designazione a Responsabile/sub-Responsabile del trattamento, da parte dell'Amministrazione, relativamente ai dati personali di cui la stessa è Titolare e che potranno essere trattati dal Fornitore nell'ambito dell'erogazione dei servizi contrattualmente previsti.
7. Nel caso in cui il Fornitore violi gli obblighi previsti dalla normativa in materia di protezione dei dati personali, o nel caso di nomina a Responsabile/sub-Responsabile, agisca in modo difforme o contrario alle legittime istruzioni impartitegli dal Titolare, oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento, risponderà integralmente del danno cagionato agli "interessati". In tal caso, l'Amministrazione potrà applicare le penali eventualmente previste nell'Accordo Quadro, e potrà risolvere il Contratto esecutivo ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno. L'Amministrazione dovrà segnalare la fattispecie alla Consip S.p.a. che potrà risolvere l'Accordo Quadro.

8. Il Fornitore si impegna ad osservare le vigenti disposizioni in materia di sicurezza e riservatezza dei dati personali e a farle osservare ai propri dipendenti e collaboratori, quali persone autorizzate al trattamento dei Dati personali.
9. In conformità a quanto previsto dal Regolamento UE/2016/679, il Fornitore dovrà garantire che i dati personali oggetto di trattamento, verranno gestiti nell'ambito dell'UE e che non sarà effettuato alcun trasferimento degli stessi verso un paese terzo o un'organizzazione internazionale al di fuori dell'UE o dello Spazio Economico Europeo, fatta eccezione dei paesi/territori/organizzazioni coperti da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 Regolamento UE/2016/679 o da altre garanzie adeguate di cui agli artt. 46 e ss. del Regolamento stesso (es. utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR). Al di fuori delle predette eccezioni, il Fornitore dovrà garantire che le eventuali piattaforme/server su cui transitino i suddetti dati abbiano sede nell'UE e che qualunque replica dei dati non sia trasmessa al di fuori della UE o dello Spazio Economico Europeo.

   Nel caso di servizi di assistenza/manutenzione da remoto il cui espletamento implichi comunque il trasferimento al di fuori dell'UE di tracciati di dati connessi al servizio stesso, gli eventuali dati personali contenuti nel tracciato devono essere opportunamente anonimizzati a cura del Fornitore.

   Nel caso in cui all'esito di eventuali verifiche, ispezioni e audit effettuati dalla amministrazione contraente in qualità di titolare del trattamento, dovessero risultare trasferimenti di dati extra-ue in assenza delle adeguate garanzie di cui sopra, l'amministrazione diffiderà il responsabile del trattamento all'immediata interruzione del trasferimento di dati non autorizzato. in caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'amministrazione ne darà comunicazione al garante della privacy e potrà, in ragione della gravità della condotta del fornitore e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto esecutivo ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

ARTICOLO 24 - CODICE ETICO – MODELLO DI ORGANIZZAZIONE E GESTIONE EX D.LGS. N. 231/2001 - PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA

1. Il Fornitore dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A.
2. Il Fornitore, per effetto della sottoscrizione del presente Accordo Quadro, promettendo anche il fatto dei propri dipendenti e/o collaboratori, si impegna: (i) ad operare nel rispetto dei principi e delle previsioni di cui al D. Lgs. n. 231/2001; (ii) ad uniformarsi alle previsioni contenute nel Modello di organizzazione, gestione e controllo adottato dalla Consip S.p.A. ai sensi della D.Lgs. n. 231/2001 per le parti di pertinenza del Fornitore medesimo nonché del Codice etico e del Piano triennale per la prevenzione della corruzione e della trasparenza per le parti di pertinenza del Fornitore medesimo.
3. In caso di inadempimento da parte del Fornitore agli obblighi di cui ai precedenti commi, la Consip S.p.A., fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolta di diritto il presente Accordo Quadro.

ARTICOLO 25 - TRACCIABILITÀ DEI FLUSSI FINANZIARI

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 rispetto ai Contratti esecutivi.

2. Ferme restando le ulteriori ipotesi di risoluzione previste nel presente atto, si conviene che, in ogni caso, le Amministrazioni, 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, risolveranno di diritto, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., i Contratti esecutivi nell'ipotesi in cui le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri documenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora A.N.AC.) n. 8 del 18 novembre 2010.
3. In ogni caso, si conviene che Consip S.p.A., senza bisogno di assegnare previamente alcun termine per l'adempimento, si riserva di risolvere di diritto il presente Accordo Quadro, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., nell'ipotesi di reiterati inadempimenti agli obblighi di cui al precedente comma.
4. Il Fornitore è tenuto 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.
5. Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, ad inserire nei contratti eventualmente sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, una 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.
6. Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui all'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i è tenuto a darne immediata comunicazione a Consip S.p.A., all'Amministrazione e alla Prefettura – Ufficio Territoriale del Governo della Provincia ove ha sede la stazione appaltante.
7. 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.
8. Consip S.p.A. verificherà che nei contratti di subappalto sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale il subappaltatore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge. Con riferimento ai contratti di subfornitura, il Fornitore si obbliga a trasmettere alla Consip e all'Amministrazione, oltre alle informazioni di cui all'art. 105, comma 2, quinto periodo, del D. Lgs. n. 50/2016, anche apposita dichiarazione resa ai sensi del d.P.R. n. 445/2000, attestante che nel relativo sub-contratto, ove predisposto, sia stata inserita, a pena di nullità assoluta, un'apposita clausola con la quale il subcontraente assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge, restando inteso che la Consip e/o le Amministrazioni, si riserva di procedere a verifiche a campione sulla presenza di quanto attestato, richiedendo all'uopo la produzione degli eventuali sub-contratti stipulati, e, di adottare, all'esito dell'espletata verifica ogni più opportuna determinazione, ai sensi di legge e di contratto.
9. Ai sensi della Determinazione dell'Autorità per la Vigilanza sui contratti pubblici (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.

ARTICOLO 26 - SUBAPPALTO

1. Il Fornitore, conformemente a quanto dichiarato in sede di Offerta si è riservato di affidare in subappalto, l'esecuzione delle seguenti prestazioni:
   - Security Strategy;
   - Vulnerability Assessment;
   - Testing del codice – Statico;
   - Testing del codice – Dinamico;
   - Testing del codice – Mobile;
   - Supporto all'analisi e gestione degli incidenti;
   - Penetration Testing;
   - Compliance normativa;

   per una quota pari al 50% dell'importo contrattuale.
2. Il subappalto, ove dichiarato in sede di offerta, sarà regolato da quanto previsto dall'art. 105 del Codice nonché dai successivi commi.
3. L'Impresa si impegna a depositare presso la Consip, 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 dal Bando 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) la 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, iv) certificazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione prescritti dal D. Lgs. n. 50/2016 e s.m.i. per l'esecuzione delle attività affidate.
4. Resta inteso che l'Impresa si impegna ad inserire, nel contratto di subappalto e negli altri subcontratti, una clausola che preveda il rispetto degli obblighi di cui al Patto di Integrità da parte dei subappaltatori/subcontraenti, e la risoluzione, ai sensi dell'art. 1456 c.c., del contratto di subappalto e/o degli altri subcontratti, nel caso di violazione di tali obblighi da parte di questi ultimi; l'Impresa dovrà dare tempestiva comunicazione a Consip dell'intervenuta risoluzione.
5. In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, la 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 sub-appalto, che ricomincerà a decorrere dal completamento della documentazione.
6. 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 la Consip revocherà l'autorizzazione.
7. 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.
8. 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 presente procedura di affidamento.
9. Per le prestazioni affidate in subappalto:

A. 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;
B. devono essere corrisposti i costi della sicurezza e della manodopera, relativi alle prestazioni affidate in subappalto, alle imprese subappaltatrici senza alcun ribasso.

10. 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.
11. Il subappalto non comporta alcuna modifica agli obblighi e agli oneri del Fornitore, il quale rimane l'unico e solo responsabile, nei confronti della Consip S.p.A. e/o delle Amministrazioni Contraenti, per quanto di rispettiva competenza, della perfetta esecuzione del contratto anche per la parte subappaltata.
12. Il Fornitore è responsabile in via esclusiva nei confronti della Consip e delle Amministrazioni Contraenti dei danni che dovessero derivare, alla Consip e alle Amministrazioni contraenti o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività. In particolare, il Fornitore si impegna a manlevare e tenere indenne la Consip S.p.A. e/o le Amministrazioni Contraenti 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 UE n. 2016/679.
13. 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 alla Consip e 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, l'Amministrazione contraente acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.
14. L'aggiudicatario 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 e s.m.i..
15. 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 e s.m.i..
16. 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.
17. Nelle ipotesi di inadempimenti da parte dell'impresa subappaltatrice, ferma restando la possibilità di revoca dell'autorizzazione al subappalto, è onere del Fornitore svolgere in proprio le attività ovvero porre in essere, nei

confronti del subappaltatore ogni rimedio contrattuale, ivi inclusa la risoluzione.

18. L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.
19. In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti comma, la Consip e l'Amministrazione contraente possono risolvere l'AQ e il Contratto esecutivo, salvo il diritto al risarcimento del danno.
20. Solo nel caso in cui sia presente nel disciplinare di gara la clausola che vieta la partecipazione dei cd. RTI sovrabbondanti, la Consip non autorizzerà il subappalto nei casi in cui l'impresa subappaltatrice possieda singolarmente i requisiti economici e tecnici che le avrebbero consentito la partecipazione alla gara.
21. Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016 e s.m.i., il Fornitore si impegna a comunicare alla Consip S.p.A., prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione dell'Accordo Quadro, 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.
22. 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 dell'Accordo Quadro e devono essere depositati alla Consip prima o contestualmente alla sottoscrizione dell'accordo Quadro.
23. 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.
24. La Consip S.p.A., 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.

ARTICOLO 27 - DANNI E RESPONSABILITÀ CIVILE

1. Il Fornitore assume in proprio ogni responsabilità per qualsiasi danno causato a persone o beni, tanto del Fornitore stesso quanto delle Amministrazioni Contraenti e/o della Consip S.p.A. e/o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze relative all'esecuzione delle prestazioni che discendono dall'Accordo Quadro e ad esso riferibili, anche se eseguite da parte di terzi.

ARTICOLO 28 - ONERI FISCALI E SPESE CONTRATTUALI

1. Sono a carico del Fornitore tutti gli oneri tributari e le spese contrattuali ivi comprese quelle previste dalla normativa vigente relative all'imposta di bollo.
2. Laddove la registrazione sia operata dalla Consip S.p.A. e/o dalle Amministrazioni Contraenti, le stesse comunicano al Fornitore l'importo anticipato e il conto corrente sul quale il Fornitore si impegna a versare, entro dieci giorni, l'importo anticipato. L'attestazione del versamento deve essere prodotta a Consip S.p.A. e/o alle Amministrazioni Contraenti entro venti giorni dalla data in cui è effettuato. In caso di ritardo l'importo è aumentato degli interessi legali a decorrere dalla data di scadenza del suddetto termine fino alla data di effettivo versamento.
3. Il Fornitore dichiara che le prestazioni di cui trattasi sono effettuate nell'esercizio di impresa e che trattasi di operazioni soggette all'Imposta sul Valore Aggiunto, che il Fornitore – salvo il caso di applicazione dell'art. 17-ter del d.P.R. n. 633 del 1972 introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96 ("split payment") - è tenuto a versare, con diritto di rivalsa, ai sensi del D.P.R. n. 633/72; conseguentemente, all'Accordo Quadro dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'articolo 40 del D.P.R. n. 131/86, con ogni relativo onere a carico del Fornitore.

ARTICOLO 29 - CONTRIBUTO A CARICO DELLE AMMINISTRAZIONI

1. 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.
2. Pertanto, le Amministrazioni contraenti sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del 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 Contratto esecutivo, determinato sulla base del Piano Operativo approvato dall'Amministrazione Beneficiaria all'atto della stipula del Contratto esecutivo medesimo.
3. 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 contraente ai sensi del precedente articolo 6, 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.
4. Le modalità operative di pagamento del predetto contributo sono rese note alle Amministrazioni contraente a mezzo di apposita comunicazione sul sito internet della Consip S.p.A. (www.consip.it).

   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.

ARTICOLO 30 - CLAUSOLA FINALE

1. Il presente Accordo Quadro ed i suoi Allegati costituiscono manifestazione integrale della volontà negoziale delle parti che hanno altresì preso piena conoscenza di tutte le relative clausole, avendone negoziato il contenuto, che dichiarano quindi di approvare specificamente singolarmente nonché nel loro insieme e, comunque, qualunque modifica al presente atto ed ai suoi Allegati non potrà aver luogo e non potrà essere provata che mediante atto scritto; inoltre, l'eventuale invalidità o inefficacia di una delle clausole dell'Accordo Quadro e/o dei singoli Contratti esecutivi non comporta l'invalidità o inefficacia dei medesimi atti nel loro complesso.
2. Qualsiasi omissione o ritardo nella richiesta di adempimento dell'Accordo Quadro o dei singoli Contratti esecutivi (o di parte di essi) da parte di Consip S.p.A. e/o delle Amministrazioni non costituisce in nessun caso rinuncia ai diritti loro spettanti che le medesime si riservano comunque di far valere nei limiti della prescrizione.
3. Con il presente Accordo Quadro si intendono regolati tutti i termini generali del rapporto tra le Parti; in conseguenza esso non verrà sostituito o superato dai Contratti esecutivi o integrativi dell'Accordo Quadro che sopravvivrà ai detti Contratti esecutivi continuando, con essi, a regolare la materia tra le Parti.

ART. 31 – PENDENZA TERMINE APPELLO SU SENTENZA TAR LAZIO

1. Atteso che, la stipula avviene in pendenza del termine per la proposizione dell'appello avverso la sentenza del TAR Lazio Roma n. 04840/2022, che ha confermato la piena legittimità del provvedimento di aggiudicazione disposto

dalla Consip S.p.A. in favore del Fornitore e che, dalla proposizione di tale gravame potrebbe derivare un eventuale e futuro provvedimento giurisdizionale e/o amministrativo relativo a ulteriori e diversi giudizi o procedimenti di qualsivoglia natura che dovessero essere instaurati da chicchessia – qualora dovesse essere imposto il riesame e/o l'annullamento, anche in autotutela, dell'aggiudicazione definitiva e/o della gara e da ciò scaturisse qualsiasi tipo di invalidità e/o perdita di efficacia del contratto, il Fornitore con la sottoscrizione del contratto espressamente rinuncia, ora per allora, irrevocabilmente ed a titolo definitivo, a proporre successive azioni e/o eccezioni volte ad ottenere un risarcimento del danno nei confronti della stazione appaltante. Restano salvi ed impregiudicati i diritti del Fornitore all'impugnativa dei provvedimenti giudiziali e/o amministrativi che lo vedessero soccombente nei procedimenti giudiziari di cui sopra.

Roma, lì ___ ___

CONSIP S.p.A. **IL FORNITORE**

_____ _____

Il sottoscritto, nella qualità di legale rappresentante del Fornitore, dichiara di avere particolareggiata e perfetta conoscenza di tutte le clausole contrattuali e dei documenti ed atti ivi richiamati; ai sensi e per gli effetti di cui agli artt. 1341 e 1342 cod. civ., il Fornitore dichiara di accettare tutte le condizioni e patti ivi contenuti e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni di seguito elencate:

Articolo 3 (Oggetto dell'Accordo Quadro), Articolo 4 (Durata dell'Accordo Quadro e dei Contratti esecutivi), Articolo 5 (Prezzi e vincoli dei Contratti esecutivi), Articolo 6 (Affidamento dei Contratti esecutivi), Articolo 7 (Obbligazioni generali del Fornitore), Articolo 8 (Obbligazioni specifiche del Fornitore), Articolo 9 (Verifica di conformità), Articolo 10 (Corrispettivi e fatturazione), Articolo 11 (Costi della sicurezza); Articolo 12 (Penali); Articolo 13 (Garanzie); Articolo 14 (Risoluzione); Articolo 15 (Recesso); Articolo 16 (Obblighi derivanti dal rapporto di lavoro), Articolo 17 (Trasparenza), Articolo 18 (Riservatezza), Articolo 19 (Responsabile Unico delle Attività Contrattuali, Articolo 20 (Divieto di cessione del contratto), Articolo 21 (Brevetti industriali e diritti d'autore); Articolo 22 (Foro competente); Articolo 23 (Trattamento dei dati personali); Articolo 24 (Codice Etico – Modello di organizzazione e gestione ex D.Lgs. n. 231/2001 – Piano Triennale per la prevenzione della corruzione e della trasparenza), Articolo 25 (Tracciabilità dei flussi finanziari), Articolo 26 (Subappalto), Articolo 27 (Danni e responsabilità civile), Articolo 28 (Oneri fiscali e spese contrattuali), Articolo 29 (Commissione a carico delle Amministrazioni), Articolo 30 (Clausola finale), Articolo 31 (Pendenza termine appello su sentenza TAR Lazio**)**.

Roma, lì ___ ___

IL FORNITORE

ALLEGATO A – OFFERTA TECNICA DEL FORNITORE

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

Offerta Tecnica

CIG - 8884642E81

LOTTO 2

Sommario

1 Premessa

1.1 Contesto di riferimento e principi della fornitura

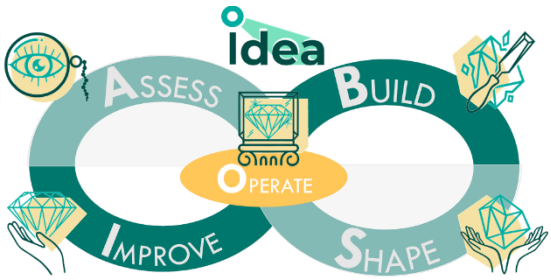
La difesa dal rischio cyber è di massima priorità in tutti i settori dell'economia, dello Stato e della società civile; lo scenario Covid poi, ha reso ancora più tangibile un'esigenza già prima impellente. La Pubblica Amministrazione è nel mirino di una minaccia sempre più sofisticata e con conseguenze sempre più gravi. Una cartella clinica può valere centinaia di euro per il cyber crime. La maggioranza delle Amministrazioni Pubbliche, per taluni analisti oltre il 60%, è vulnerabile tanto nelle tecnologie abilitanti, quanto nei processi e nelle competenze, intese nel senso più generale di capacità di orientarsi nel complesso delle conoscenze e sensibilità necessarie per operare in sicurezza nel cyber space.

La presente offerta nasce da **significative capacità ed esperienze** nel panorama professionale del settore dell'Information Technology ed in particolare nell'ambito della cybersecuity, espresse al fianco delle Pubbliche Amministrazioni Centrali e Locali.

L'intera offerta si ispira e si sostanzia per indirizzare quelli che sono - a nostro avviso - i **10 fattori critici di successo della presente fornitura** (elencati di seguito ed evidenziati ad ogni ricorrenza lungo il documento): *standardizzazione dei processi operativi* e, dove possibile, *automazione dei servizi*, finalizzata alla garanzia del risultato e alla sicurezza dell'esecuzione; *situational awareness*, attitudine nata in ambito militare, estesa negli anni a tutte le operazioni critiche (dal trasporto aereo alla gestione delle emergenze ambientali) e oggi richiamata dalle buone prassi di cyber security. Nell'offerta tale attitudine è parte dell'approccio proposto alle attività - dal presidio delle vulnerabilità alla gestione degli incidenti - e contribuisce ad un consapevole *strategy setting*; *approccio risk based*, perseguito in tutte le fasi dei servizi offerti, con l'intento di supportare l'Amministrazione nel mantenimento di un *equo rapporto tra rischio e spesa* all'interno del progetto di sicurezza, in un quadro generale di esposizione ad un crescente fabbisogno di protezione dettato dalla stretta delle normative e dalla minaccia incombente; *tailoring dei servizi*, adeguandoli alle specificità del comparto (PA centrale o locale) e della tipologia di Ente e soprattutto con la massima attenzione alla *sostenibilità degli interventi da parte dell'organizzazione*, in modo da agevolare l'applicazione della *due care* rispettando l'effettiva capacità interna; *concretezza* attraverso la proposizione di un "catalogo del riuso" (di modelli e strumenti collaudati e replicabili), che rafforzi anche l'obiettivo di standardizzazione e *velocità*; *information sharing*, pratica alla base dell'accrescimento della capacità di difesa (e velocità di risposta) contro il rischio cyber, promossa all'interno dei gruppi di lavoro, come strumento di accelerazione della knowledge base comune.

1.2 Proposta progettuale

I servizi oggetto della presente fornitura saranno erogati dal nostro raggruppamento secondo la metodologia Idea **(Intellera Digital Empowerment Accelerator)**, adottata nella Pubblica Amministrazione per il governo di progetti complessi a matrice digitale. La metodologia si compone di **4 fasi sequenziali (Assess, Shape, Build, Improve)** volte a tracciare un percorso di erogazione coerente con i servizi del Lotto 2, e di **una fase continuativa** (Operate) finalizzata al monitoraggio e al supporto operativo alle Amministrazioni. Nel dettaglio:



- **ASSESS:** declinazione degli obiettivi del servizio in priorità; analisi e valutazione del contesto operativo e del grado di maturità; individuazione delle criticità e delle aree di miglioramento;
- **SHAPE:** individuazione e macro-disegno delle soluzioni da implementare con evidenza del piano di azione, delle responsabilità, dei tempi e degli strumenti da utilizzare;
- **BUILD:** costruzione e prima adozione delle soluzioni individuate; raccolta delle evidenze circa gli output delle soluzioni ed analisi dell'efficacia delle stesse;
- **IMPROVE:** fine-tuning delle soluzioni, supporto all'adozione da parte degli utenti, valutazione dell'impatto delle soluzioni e costruzione delle lesson learned dell'iniziativa;
- **OPERATE:** durante la quale, a conclusione della fase progettuale, con un approccio di **Continuous Improvement**, vengono portate avanti attività di monitoraggio e supporto operativo.

Di seguito è riportata la leggenda dei "segna posto" utili per identificare rapidamente nel testo gli aspetti legati a metodologia, competenze tematiche, strumenti, soluzioni tecnologiche:

- Quando si menziona un obiettivo specifico per l'erogazione dei servizi
- Quando si menziona una metodologia da adottare per l'erogazione dei servizi
- Quando si menziona uno standard da adottare per l'erogazione dei servizi
- Quando si menziona uno strumento o una soluzione tecnologica da adottare per l'erogazione dei servizi
- Quando si menzionano degli aspetti di efficacia e concretezza di una soluzione specifica per l'erogazione dei servizi

2 Presentazione e descrizione dell'offerente

Le aziende che compongono il nostro Raggruppamento sono:

Intellera Consulting (*former* PwC Public Sector) è una società di consulenza nata dal management buyout della linea di business di PwC Italia **dedicata alla Pubblica Amministrazione e all'Healthcare**; dispone di **network di circa 700 professionisti**, si configura come apripista nella consulenza strategica e direzionale, e propone servizi professionali d'eccellenza

a istituzioni, amministrazioni e imprese. Intellera svolge numerosi progetti in ambito cyber security, di diversa natura e complessità, afferenti alle PA Centrali (es: Consip, Ministero dell'Economia e Finanze, Ministero della Salute, INAIL, ecc.), a PA Locali (es: Roma Capitale, Comune di Milano, Regione Lazio, Regione Toscana, Regione Campania, Comune di Venezia, ecc.) e ad altri Enti del settore pubblico (es: AgID, Sogei, Consip, ecc.).

Capgemini è leader mondiale nella Cyber Security ed opera con più di **270.000 persone**, presenti in quasi **50 paesi** in tutto il mondo, con una forte esperienza sui principali mercati internazionale e italiano. La **Cyber Security rappresenta il core business** di Capgemini e viene sviluppata attraverso **un team globale costituito da oltre 4000** risorse con competenze qualificate che offrono un approccio a 360° su piattaforme IT, OT, cloud e IoT. Includiamo un set di servizi gestiti da personale con elevati skill in ambito di **Ethical Hacking** per fare attività di analisi delle vulnerabilità di servizi e infrastrutture delle aziende clienti.

HSPI SpA è una società di consulenza direzionale nata nel 2003, leader in Italia sulle tematiche di **IT Governance, IT Service Management, Management Consulting,** che conta più di 150 professionisti dislocati sulle tre sedi di Roma, Bologna e Milano in grado di offrire una vasta gamma di servizi professionali grazie ad un modello operativo capace di integrare competenze distintive di Consulenza Direzionale e conoscenze specialistiche in ambito ICT. HSPI ha maturato una notevole esperienza nella PA attraverso l'adozione di metodologie in linea con gli standard internazionali e alla collaborazione e partnership con associazioni internazionali ed enti per lo studio e la diffusione delle migliori pratiche di **IT Governance, IT Security e IT Service Management.**

Teleconsys è una **Digital Innovation Company** il cui principale ambito di expertise è supportare le organizzazioni pubbliche e private in tutte le fasi del loro viaggio di trasformazione digitale attraverso l'adozione dei principali **digital enabler** e dell'**open innovation**. Iscritta dal 2019 nella sezione speciale del registro delle imprese in quanto investe più del 3% del VdP in RSI, ha specifiche competenze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection e Intelligence ed è strutturata su 3 BU (Next Generation Infrastructure & Cybersecurity, Agile Application Development & UX, Intelligent Service & Operation), intersecate da due strutture di innovazione: il **Digital Innovation Experience e l'Innovation & Contamination Lab**.

La ripartizione delle attività tra le società del RTI è particolarmente funzionale all'erogazione dei servizi perché, oltre a valorizzare gli elementi di "specializzazione" di ciascun proponente, consente di **enfatizzare la complementarità delle rispettive competenze** e assicurare una chiara individuazione delle responsabilità. Con il simbolo (✓) sono indicate gli ambiti di prevalente coinvolgimento mentre con il simbolo (✓) il coinvolgimento.

Servizi fornitura – Lotto 2	Intellera Consulting	Capgemini	HSPI	Teleconsys
Security strategy	✓	✓	✓	✓
Vulnerability assessment	✓	✓	✓	✓
Testing del codice	✓	✓	✓	✓
Supporto all'analisi e gestione degli incidenti	✓	✓	✓	✓
Penetration testing	✓	✓	✓	✓
Compliance normativa	✓	✓	✓	✓

La Presente Relazione Tecnica viene sottoscritta e firmata da:

- per **Intellera Consulting Srl**: Giancarlo Senatore, [redacted], in qualità di Amministratore Delegato e legale rappresentante, e Mario Papini nato a Monza il 22/05/1969 in qualità di Amministratore;
- per **Capgemini Spa**: Andrea Falleni, [redacted] in qualità di Amministratore Delegato e legale rappresentante;
- per **HSPI Spa**: Sebastiano Manno, [redacted] qualità di Amministratore Delegato e legale rappresentante;
- per **Teleconsys Spa**: Giada Apicella, nata a [redacted] n qualità di Procuratore.

3 Struttura Organizzativa

La soluzione proposta per il governo della fornitura nasce dalla nostra conoscenza del contesto Pubblico e si basa sul paradigma **dell'Agile Program Management** affinato anche grazie alle esperienze di gestione di Accordi/Contratti Quadro Consip (SPC Lotto 3 e Lotto 4, SGI Lotto 2 e Lotto 3, AQ Servizi Applicativi Lotto 1 e 2, Convenzione AT). Tali esperienze ci hanno visti impegnati nell'erogazione di numerosi contratti esecutivi/appalti specifici **(oltre 300 gestiti in parallelo)**, anche di dimensioni rilevanti, con grande eterogeneità funzionale e dimensionale (citiamo, ad es. grandi Amministrazioni Centrali quali MEF, Ministero del Lavoro, Ministero della Salute, INPS, INAIL, Consip, AgID, Agenzia per la Cybersicurezza Nazionale -ACN- e Amministrazioni Locali quali Regione Lombardia, Regione Lazio, Comune di Milano, Roma Capitale). La soluzione organizzativa è stata definita a partire dalla identificazione delle **caratteristiche di efficacia e di concretezza** necessarie alla gestione e presidio di un Accordo Quadro "multi-Amministrazione". Di seguito saranno descritti anche i ruoli e le figure organizzative aggiuntive messe a disposizione della fornitura e indicate con il simbolo .

GOVERNO DELLA COMPLESSITÀ

Capacità di governare in maniera unitaria e sinergica dagli obiettivi strategici della fornitura agli obiettivi operativi del singolo servizio/iniziativa. **Soluzione adottata:** abbiamo definito una struttura che gestisce in maniera integrata i due ambiti operativi (Accordo Quadro

e Contratti Esecutivi) e tre livelli di governo (Strategico, Programma, Progetto). ► **Livello Strategico:** presidia la definizione, il monitoraggio e la revisione della strategia complessiva di approccio all'AQ ed i suoi obiettivi. ► **Livello di Programma:** grazie all'approccio dell'**Agile Program Management** gli obiettivi strategici vengono tradotti in modo coordinato in obiettivi specifici (contratto esecutivo) e vengono gestite risorse e pianificazione a livello centralizzato. Inoltre, al fine di garantire un efficace condivisione delle informazioni tra i diversi servizi della fornitura, istituiamo un tavolo di coordinamento – il **Security Project Board (SPB)** – nel quale parteciperanno i singoli Responsabili Tecnici di tutti i servizi. Il SPB insieme al **Board dei Fornitori** (descritto di seguito) rappresentano le strutture aggiuntive che consentiranno di garantire il coordinamento unitario dei progetti di sicurezza ► **Livello di Progetto:** A livello di contratto esecutivo, i singoli interventi vengono istanziati in soluzioni operative secondo i principi Agile (**Agile Project Management)**.

Capacità di assicurare la gestione di tutte le dimensioni manageriali di un Programma (attività, tempi, risorse, competenze, qualità, rischi) e il tailoring dei servizi. **Soluzione adottata:** sono state **istituite le seguenti strutture/figure aggiuntive** ► **Quality & Risk Office (Q&R)** responsabile della qualità e del risk management nell'AQ, interfaccia unica per i RUAC-CE dei singoli Contratti Esecutivi come SME (nei casi di necessità di escalation) e come governo e diffusione delle metodologie e standard. ► **Program Manager (PM)** responsabile del coordinamento delle iniziative e delle correlazioni tra i diversi CE. È supportato operativamente da una struttura di PMO. ► **Resource Manager (RM)** responsabile della gestione delle risorse umane in tutte le fasi dell'attuazione dei contratti esecutivi, dalla loro identificazione per il "coinvolgimento nei progetti" alla formazione e scheduling, sino al rilascio al termine delle attività. Supporta il RUAC-CE dei singoli contratti esecutivi nella gestione/sostituzione delle risorse del RTI.

ASCOLTO E COMPRENSIONE

Capacità di valorizzare le singole specificità e le esigenze degli stakeholder a tutti i livelli di governo.

Soluzione adottata: abbiamo definito **strutture aggiuntive** preposte alla raccolta, analisi e comprensione delle esigenze degli stakeholder. ► **Steering Committee (SC)**, quale tavolo di coordinamento strategico permanente per condividere indirizzi, strategie, risultati ed eventuali criticità, nonché assicurare unitarietà di visione nell'erogazione dei servizi. Al tavolo partecipano oltre al RTI anche i referenti di Consip e di altri stakeholder istituzionali impattati (referenti di Consip, AgID e ACN). ►**Technical Board (TB)**, tavolo di lavoro a cui partecipano i Referenti tecnici AgID e ACN, i referenti tecnici degli Uffici di IT security e privacy delle Amministrazioni aderenti, per condividere le metodologie applicate/best practice, le scelte tecnologiche, gli strumenti di analisi. ► **Board Fornitori (BF)**, luogo di confronto con i referenti degli aggiudicatari del Lotto 1, per supportare le Amministrazioni nella individuazione dei fabbisogni e per condividere metodologie e soluzioni a eventuali criticità, favorendo l'uniformità e la standardizzazione degli interventi.

Capacità di intercettare la conoscenza e le innovazioni sia tecniche che regolamentari che si generano sul mercato e di trasferirle alle risorse dell'organizzazione. **Soluzione adottata:** sono state istituite **le seguenti strutture/figure aggiuntive** ► **Osservatorio Normativo sulla Security & Privacy (ONS&P)** rappresenta la struttura deputata all'analisi e studio della normativa in via di evoluzione sui temi di sicurezza e privacy, fornendo elementi utili per l'applicazione concreta nell'ambito dei CE. ► **Security & Privacy Enabler Solution Innovators (SPESI)** è una unità organizzativa volta a valorizzare le soluzioni innovative in tema di sicurezza prodotte dalla PMI innovativa e dai nostri centri di competenza. ► **Knowledge Manager (KM)** è la figura incaricata della gestione del know-how della Fornitura (es. presa in carico, condivisione di best practice e lesson learned, ecc.). Supporta le attività di condivisione documentale all'interno del Portale della Fornitura.

Capacità di comprendere e, dove possibile, "anticipare" in ottica di risk based le esigenze delle Amministrazioni aderenti. **Soluzione adottata:** è stata definita una **struttura ad-hoc aggiuntiva** per la raccolta delle esigenze delle Amministrazioni denominata **Account & Demand Management Office (ADMO)**. È la struttura di raccordo tra l'ambito AQ e quello CE, centralizzando il supporto alle PA nella compilazione del Piano dei Fabbisogni/Piano Operativo. Coordina le attività dei Focal Point (descritti di seguito) nelle fasi di attivazione e di esecuzione dei CE. Coordina gli Account Territoriali (AT). Gli AT hanno il compito di promuovere l'AQ presso gli Enti potenzialmente destinatari, raccogliere e razionalizzare, secondo un equo rapporto tra rischio e spesa, le esigenze delle Amministrazione aderenti e formalizzarle in un Piano dei fabbisogni/Operativo.

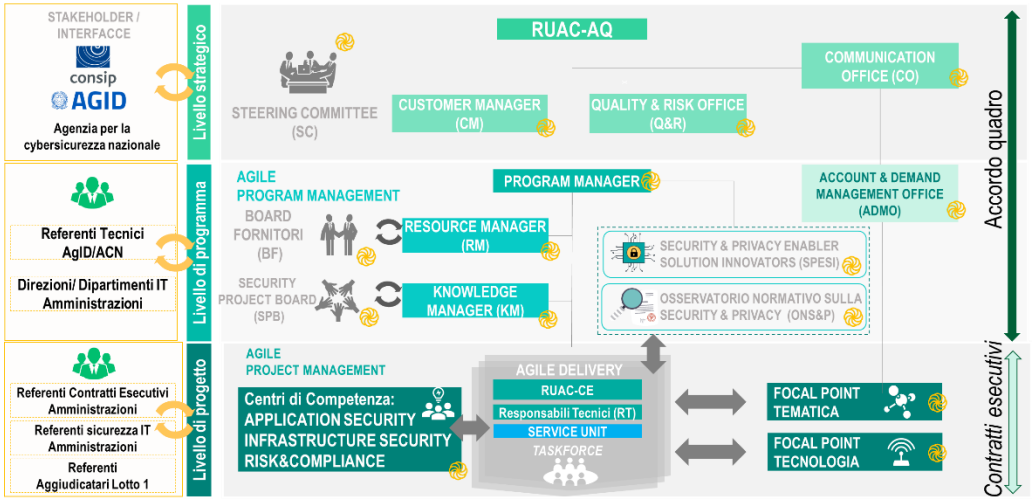
DELIVERY

Capacità di massimizzare la soddisfazione dell'Amministrazione destinataria. **Soluzione adottata:** abbiamo previsto una **figura aggiuntiva dedicata** alla cura della soddisfazione delle Amministrazioni e degli altri stakeholder (tra cui AgID e Agenzia per la cybersicurezza nazionale) denominata **Customer Manager (CM)**. Il CM raccoglie e analizza le segnalazioni delle Amministrazioni presidiando il mantenimento delle aspettative e dei livelli di qualità attesi, informando i singoli RUAC-CE su eventuali criticità da gestire. Ha la responsabilità della gestione del Portale della fornitura e dei canali di comunicazione digitali (es.: social media), e cura la creazione di contenuti di qualità dei diversi canali comunicativi.

Capacità di massimizzare la standardizzazione dei processi operativi e la flessibilità nella delivery, in relazione a cambiamenti di contesto, imprevisti o modifiche delle priorità. **Soluzione adottata:** attraverso l'approccio **Agile Project Delivery** tutte le competenze necessarie all'erogazione dei servizi sono sempre garantite nell'ambito dei Team Agile, assicurando adattabilità e flessibilità all'eterogeneità dei progetti, anche attraverso la capacità di monitoraggio e pronta risposta a picchi di attività, esigenze ad hoc e specificità territoriali.

Capacità di assicurare in termini quantitativi e qualitativi le risorse necessarie per l'esecuzione dei servizi della fornitura. **Soluzione adottata:** ogni ambito di natura tecnica e regolamentare è presidiato dai **Focal Point**, ovvero risorse con elevatissima specializzazione di tematica e tecnologia e almeno 15 anni di esperienza appartenenti alla struttura di ADMO, che assicurano il costante collegamento con i centri di Competenza e Delivery per lo staffing dei team di lavoro.

Nella figura seguente viene rappresentato **l'organigramma dell'organizzazione** nella sua interezza, dedicata per la gestione dell'Accordo Quadro e dei Contratti Esecutivi. Con il simbolo sono indicati i ruoli e le figure organizzative aggiuntive messe a disposizione della fornitura.



Nella cornice di tale struttura, **le società del nostro raggruppamento hanno delle responsabilità specifiche ma fortemente complementari rispetto a tutti gli ambiti/servizi oggetto di Fornitura.** In particolare:

Intellera Consulting Srl, in qualità di mandataria, garantirà il governo dell'AQ e sarà responsabile dell'erogazione di tutti i servizi richiesti. Grazie all'esperienza nell'ambito del public IT security & privacy, avrà un ruolo guida nell'ambito dei servizi di Security Strategy e di Compliance Normativa, nonché nel supporto alle Amministrazioni nell'analisi degli impatti e nell'implementazione concreta degli adempimenti dettati dal GDPR con un focus specifico al perimetro IT.

Capgemini Spa metterà a disposizione delle Amministrazioni destinatarie le sue competenze e professionalità tecniche maturate nella PA a tutti i livelli di governo sui temi IT e IT Security. Nell'ambito della fornitura avrà un ruolo prioritario nell'ambito dei servizi di vulnerability assessment, testing del codice, penetration testing e analisi e gestione degli incidenti.

HSPI Spa avrà un ruolo fondamentale nel supportare le PA nella strutturazione dei progetti di sicurezza, mettendo a disposizione le competenze per i servizi di Security Strategy, con un focus sull'advisory sulle soluzioni di beni e servizi in materia di IT Security.

Teleconsys Spa è una **PMI Innovativa** con specifiche competenze ed esperienze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection. Avrà un ruolo fondamentale nel supportare le PA nell'individuazione di soluzioni innovative e "best in class" di sicurezza e di rinnovamento tecnologico, in maniera trasversale rispetto ai servizi oggetto della fornitura.

Per garantire il **coordinamento tra le diverse strutture organizzative e le modalità di interazione con le Amministrazioni destinatarie**, proponiamo un **modello operativo basato su processi standard e azioni di condivisione strutturati**.

Promozione AQ: gli Account Territoriali (AT) promuovono in modalità proattiva l'AQ presso le Amministrazioni target del proprio ambito territoriale di riferimento, attraverso: ► **sessioni di promozione** con i Referenti di sicurezza IT e privacy delle PA, al fine di illustrare gli ambiti di applicazione dell'AQ e fornire informazioni per attivare i CE; ► **eventi tematici** o partecipazione a eventi esterni.

Definizione CE: il RUAC-CE, con il supporto del ADMO e del RKM, coordina le azioni per accompagnare le PA dal primo contatto fino alla stipula dei CE, anche attraverso la pianificazione di una serie di incontri con i diversi Referenti IT e di privacy dell'Amministrazione aderente.

Esecuzione e monitoraggio CE: le strutture aggiuntive di Technical Board e l'Osservatorio Normativo sulla Security & Privacy garantiscono il coordinamento interno in termini di aderenza agli standard e di aggiornamento rispetto alle evoluzioni che potranno verificarsi nel corso della fornitura, supportando i GdL anche attraverso pillole formative o incontri di approfondimento. Il PM è responsabile della coerenza e della sostenibilità di tutti gli interventi progettuali tramite una vista unitaria, organizzando incontri di allineamento e monitoraggio con i singoli RUAC-CE. Infine, la struttura aggiuntiva **Security & Privacy Enabler Solution Innovators (SPESI)** si interfaccia con le Amministrazioni, secondo un duplice approccio: "push", offrendo una vasta gamma di possibili interventi di potenziamento di beni e servizi di sicurezza innovativi e di frontiera, anche ricercando nuovi filoni di intervento; "pull", efficientando le tempistiche di risposta a vincoli normativi sfidanti.

Creazione e animazione della Learning & Working Security Community: proponiamo di attivare un modello di condivisione della conoscenza che consenta di regolare l'*Information Sharing* e attivare meccanismi virtuosi di trasferimento e spill-over. A tal proposito, proponiamo l'istituzione di una **Learning & Working Security Community (L&WSC)**, una community professionale costituita da tutti gli attori che intervengono nei progetti di sicurezza IT. La L&WSC è un luogo dell'apprendimento in grado di produrre innovazione e miglioramenti continui. La L&WSC opererà su tre livelli di responsabilità: ► **I livello**: è composto dai referenti delle PA (Referenti della sicurezza IT e Referenti della privacy) che svolgono la funzione di anello di congiunzione fra i decision maker, i Fornitori e eventualmente i cittadini/utenti. Hanno il compito realizzare e monitorare i progetti di sicurezza; ► **II livello**: vi fanno parte i Fornitori aggiudicatari dei due lotti ed hanno un ruolo chiave nell'analisi/ascolto dei fabbisogni e nella attuazione dei servizi. La L&WSC è attivata attraverso

modalità in presenza (focus group, riunioni, workshop) e modalità a distanza descritti al paragrafo Portale della Fornitura. ► **III livello:** è rappresentato dai cittadini/utenti dei servizi interessati dai progetti di sicurezza e ha un ruolo fondamentale nella valutazione ex-post dei risultati raggiunti.

Inoltre, ad accompagnare tale modello operativo, saranno messi a disposizione della presente fornitura un **set di strumenti di condivisione delle informazioni** già ampiamente sperimentati in Accordi/Contratti Quadro analoghi:

ATTIVITÀ	DESCRIZIONE	PERIODICITÀ	RUOLI COINVOLTI
Incontri di avanzamento AQ	Convocati dal RUAC-AQ, coinvolgendo il SC, per condividere l'andamento della fornitura, la definizione di azioni propositive nei confronti di AgID, ACN e delle PA.	Bimestrale o ad eventi significativi	RUAC-AQ, SC
SAL Programma	Convocati dal PM per coordinare e monitorare la gestione integrata delle attività, la dimensione e mix dei team sui singoli CE facilitando l'integrazione tra iniziative	Bimestrale o ad eventi significativi	RUAC-AQ, PM, PMO, RKM, ADMO
SAL di CE/Progetto di sicurezza	Convocati dal RUAC-CE, coinvolgendo il SPB e il BF, per verificare l'andamento delle attività dello specifico Contratto Esecutivo/progetto di sicurezza	Ad hoc	RUAC-CE, SPB, BT, ADMO, Referenti Amm.
SAL di Servizio	Riunioni ad hoc sull'andamento delle attività dello specifico servizio, attivati dai RT	Mensile o ad hoc	RT, GdL – Referenti Amm.
Meeting tecnici interni	Organizzati per discutere di specifici argomenti: nuove esigenze di natura normativa e tecnica, criticità, picchi di lavoro; creano sinergie informative ed operative tra i diversi team.	Mensile o ad eventi significativi	RT, FP, GdL, SPESI, ONS&P
Piano di comunicazione	Questo documento a livello di Accordo Quadro presenta l'andamento delle attività e i principali ambiti attivati anche a supporto di AgID e ACN.	Trimestrale	RUAC-AQ, PM, PMO
Documenti Operativi	Il RTI adotta standard documentali comuni a tutti i progetti/programma: Gantt, project health check, iussue log, risk log, meeting agenda, Sal, …	NA	Tutte le risorse

4 Proposta progettuale per il servizio "Security Strategy"

"E' con la scelta di strategie adatte che problemi complicati vengono ridotti a semplici fenomeni e poi risolti"
(Charles Proteus Steinmetz)

Obiettivi del servizio: supportare le PA nella definizione del Progetto di sicurezza e dei relativi fabbisogni di beni e servizi, assicurando: ► **una chiara definizione degli obiettivi di sicurezza** (Security Target Profile); ► **l'identificazione dei gap da colmare** rispetto alla situazione di partenza (Security Current Profile); ► **la definizione di una roadmap strategica** degli interventi da implementare; ► la traduzione degli interventi in un **piano dei fabbisogni** di beni e servizi; ► **una chiara identificazione dei ruoli** e delle responsabilità di governo e di gestione di tutte le fasi.

L'elaborazione del Progetto di Sicurezza è quindi il procedimento grazie al quale vengono definite le scelte strategiche di governo e gestione della sicurezza delle informazioni e delle azioni implementative da avviare per tutti i servizi. La nostra proposta ha come riferimento il Framework Nazionale per la **Cybersecurity e la Data Protection** (anche noto come Framework Nazionale 2.0), e si basa su un *approccio risk based* che si declina in attività seguendo **l'approccio metodologico** Idea (*cfr. § 1.2 Proposta progettuale*).

Metodologia: L'approccio metodologico proposto è strutturato come segue:

Analisi: di tutte le dimensioni (domini) da considerare nel Progetto di Sicurezza: **Strategia e Governo della Sicurezza delle Informazioni**, **Cyber Security Operation, Awareness, Gestione Eventi e Incident, Architetture di Sicurezza, Compliance Normativa** qualificandone i sotto domini (es. Formazione e Sensibilizzazione all'interno del dominio Awareness). Per la qualificazione di questi elementi la nostra proposta prevede un *approccio risk based* (analisi dei rischi cyber e dello stato rispetto a questi) al fine di tracciare così il ***Security Current Profile***.

Definizione del Modello: attraverso interviste e workshop con i referenti chiave della Amministrazione e benchmark con realtà analoghe, viene definito il **Modello di Gestione della Sicurezza** dell'Amministrazione e per tutti i domini e sottodomini individuati vengono declinati gli obiettivi da raggiungere, definendo il ***Security Target Profile*** dell'Amministrazione.

Pianificazione: vengono identificati i gap (es. l'assenza di un processo di Incident Management), e le aree di miglioramento (in questo caso una cultura del rischio non consolidata), elaborando la roadmap strategica e identificando le azioni da pianificare (in questo caso l'ottenimento della certificazione ISO 27001), le priorità, i risultati attesi. In questa fase viene definito il ***Modello Organizzativo di gestione della sicurezza***.

Realizzazione: grazie a tecniche tipiche del project management (es. studi di fattibilità, analisi di impatto, Portfolio Management, Business Case, PBS, WBS) la roadmap strategica viene declinata nel ***Piano dei fabbisogni di beni e servizi***, assicurandone la effettiva realizzabilità e "*sostenibilità*" economica.

Gestione e Monitoraggio: gestione e monitoraggio della implementazione del Progetto di Sicurezza, e fine tuning in un'ottica di miglioramento continuo.

Standard adottati: la metodologia si basa sugli standard nazionali ed internazionali in materia ed in particolare, come anticipato, sul Framework Nazionale 2.0; nei singoli domini (Governance, Incident, ecc), la metodologia adotta specifici standard di riferimento: es. ISO 27001; ISO 22301, Security HealthCheck dell'Information Security Forum, linee guida AgID (es. Linea Guida per la sicurezza nel procurement ICT e per lo sviluppo del software sicuro).

Strumenti a supporto: **Intellera Security Assessment Tool (ISAT)**. Repository cloud-based integrato con il Portale della Fornitura utile a guidare le attività di assessment e l'analisi dei risultati, e supportare l'elaborazione/implementazione del Progetto di Sicurezza. Lo strumento integra funzionalità di benchmarking capitalizzando, in **maniera del tutto anonima**, la knowledge maturata dal RTI in progetti di Security, consentendo la valutazione facilitata del livello di maturità dell'Amministrazione ("Security Current Profile") rispetto ad altre PA simili per caratteristiche (comparto, dimensione, modalità di gestione della tematica sicurezza, ecc). ISAT supporta anche la fase di definizione del "Security Target Profile", avvalendosi di cataloghi dei rischi e di azioni di mitigazione anch'essi costruiti in base alle esperienze maturate e fruibili come acceleratori. Affiancato a ISAT il RTI dispone dell'**Intellera Risk Knowledge Base** che si arricchisce dei report nazionali e internazionali sui trend dei rischi cyber assicurando così la disponibilità della conoscenza ai centri di competenza (Application Security, Infrastructure Security, Risk & Compliance).

4.1 Approccio proposto per l'elaborazione del "Progetto di sicurezza"

Disponiamo di un Security framework di riferimento per la rappresentazione di **Modelli di Gestione della Sicurezza** adeguati alle caratteristiche delle diverse realtà della PA. Il framework (rappresentato in figura) è da considerarsi una base di partenza, ma **può essere personalizzato** sulle base delle caratteristiche dell'Amministrazione favorendo così al tempo stesso la *velocità d'azione* e la *personalizzazione degli interventi* nei domini (es. Strategia e Governo della Sicurezza delle Informazioni) e sotto-domini (es. Policy e Procedure, Sistema di Monitoraggio, ecc.). Per ogni dominio e sotto-dominio sono predisposte checklist di valutazione a supporto delle analisi. Nel caso di PA di piccole dimensioni, il Modello viene definito in un minor numero di sotto-domini attraverso aggregazioni.

Sulla base della tipologia di Amministrazione (comparto, servizi, dimensione, ecc.) e approccio alla sicurezza, l'**ISAT** supporta i team nella realizzazione dei deliverables fondamentali quali: ① **Qualificazione e disegno del Modello di Gestione della Sicurezza** più adatto alla tipologia di PA aderente, al suo contesto operativo e alle sue capacità e competenze strutturali; ② **Definizione del Security Current Profile** e del ③ **Definizione del Security Target Profile** attraverso le analisi sul campo supportate da checklist, benchmark e analisi di impatto. Confrontando il Security Current Profile e il Security Target Profile vengono evidenziati **i gap** rispetto al Modello di Gestione della Sicurezza atteso, ④ **identificati gli interventi da effettuare** e ⑤ **articolata la Roadmap di attuazione della strategia** al fine di definire il ⑥ **Piano dei fabbisogni di beni e servizi.**

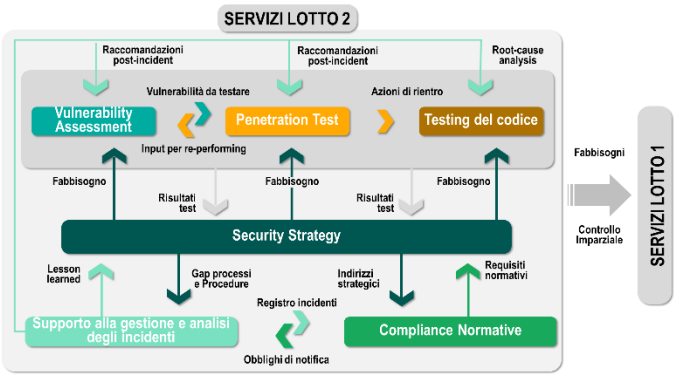
Le valutazioni vengono effettuate secondo un *approccio risk based* consentendo quindi **l'identificazione degli interventi (gap)** in base agli "obiettivi sui rischi" che si vogliono raggiungere (Security Target Profile) e la **sostenibilità** degli stessi (sia in termini di beneficio che di fattibilità) anche utilizzando la leva temporale (nel breve, medio e lungo periodo). La metodologia proposta capitalizza le tecniche tipiche del project management (es. Business Case, Product Breakdown Structure – PBS, Work Breakdown Structure-WBS) per individuare qualitativamente e quantitativamente i fattori abilitanti degli interventi, in termini di risorse necessarie e per **articolare gli interventi** della roadmap strategica in **fabbisogni di beni e servizi da approvvigionare**.

La articolazione correlata dei 6 elementi sopra illustrati, compone **il Progetto di Sicurezza della Amministrazione**. Il percorso di costruzione del Progetto di Sicurezza include, dove necessario, la redazione di studi di fattibilità, analisi di impatto, valutazione dei processi di trasformazione digitale e adeguamento al Cloud, aggiornando politiche, tassonomie e classificazioni necessarie ad indirizzare i cambiamenti nei processi di gestione.

Aspetti di correlazione con gli altri servizi

Il **Progetto di Sicurezza** indirizza dal punto di vista strategico tutti i servizi sia del Lotto 1 che del Lotto 2 e valorizza sia in input che in output tutte le informazioni prodotte nell'ambito degli altri servizi della fornitura. A livello operativo, per garantire un'efficace condivisione e coerenza delle informazioni tra i diversi servizi di gara, nella struttura organizzativa (*cfr. § 3 Struttura Organizzativa*), abbiamo inserito il **Security Project Board – SPB** (al quale

partecipano i Responsabili Tecnici dei servizi del Lotto 2) ed il **Board Fornitori - BF** (che include i referenti del Lotto 1). Tali board definiscono le modalità di *information sharing* sia in forma automatizza sia on-demand. In particolare (come evidenziato nella figura a fianco) i principali **Processi e flussi di informazioni** che il servizio di Security Strategy riceve in input dagli altri servizi del Lotto sono: ► **i risultati dei test** derivanti dalle attività di **Vulnerability Assessment, Penetration Test e Testing del codice** ► **i requisiti normativi e lesson learned** dai servizi di **Supporto all'analisi e gestione degli incidenti e Compliance normativa**. In output invece il Servizio di Security Strategy fornisce agli altri servizi: ► **gli indirizzi strategici e di coordinamento** allineati con le linee guida, le direttive e normative a livello nazionale ed europeo ► il **Piano dei fabbisogni di beni e servizi** per la realizzazione dei servizi del Lotto 1 e del Lotto 2, ed una ► **il modello di gestione della sicurezza**.



Valore aggiunto apportato dalla proposta in considerazione delle caratteristiche di contesto del Lotto

L'approccio metodologico descritto è particolarmente rilevante ed applicabile nel contesto dei servizi oggetto della gara in quanto garantisce: ► *conformità alla normativa e rispetto delle linee guida AGID*: l'utilizzo degli Standard nativamente integrato nelle metodologia (per i domini e sotto-domini di riferimento) assicura il costante aggiornamento degli interventi ai dettami normativi in essere per le diverse tipologie di PA ► *efficacia delle modalità di interazione* sia con i referenti della PA che, ove necessario, con terze parti (altre PA, imprese, organismi di governo e controllo, …), ► *omogeneità di approccio metodologico* per tutte le tipologie di PA servite, garantendo autoconsistenza del percorso seguito qualunque sia il contesto della PA aderente, stante l'applicazione del medesimo framework, opportunamente declinato a tutti i contesti ► *applicabilità a diversi contesti della PA* grazie alla disponibilità di modelli velocemente adattabili alle diverse realtà e di strumenti ampiamente sperimentati nel contesto pubblico ma provenienti da standard e best practice applicate in tutti i settori del mercato.

4.2 Proposta di elaborazione di un "Modello di analisi dei fabbisogni di beni e servizi di sicurezza"

Il piano dei fabbisogni esprime le necessità dell'Amministrazione rispetto al Modello di Gestione della Sicurezza che ha definito e che vuole implementare (insieme dei domini e sotto-domini con livello di maturità target). A supporto della identificazione dei fabbisogni il RTI dispone di **un modello di analisi** "mutuato" dalle metodologie tipiche del Project management per la definizione dei progetti tecnologici, che scompone gli interventi in beni e servizi necessari alla loro realizzazione. Gli interventi previsti nella Roadmap Strategica vengono qualificati in base a risultanze di **Business Case** specifici allo scopo di valutarne **l'effettiva "sostenibilità" costo/beneficio.** Successivamente, per ciascun intervento, si procede alla **definizione dei fabbisogni di beni e servizi** applicando tecniche di **PBS (Product Breakdown Structure)** e **WBS (Work Breakdown Structure)**. Inoltre, grazie all'utilizzo di **benchmark di comparto** eseguiti con il supporto dello strumento **ISAT,** i fabbisogni possono essere **confrontati** rispetto a contesti similari **anche in termini di Roadmap**. Questo approccio **assicura l'efficacia del piano** in quanto, collegando gli interventi e i fabbisogni agli obiettivi di sicurezza target, consente di adottare un linguaggio di comunicazione univoco (basato sul rischio) in ambito security all'interno della Amministrazione, con gli stakeholder esterni e con i fornitori.

Modelli di gestione della sicurezza e caratteristiche di comparto

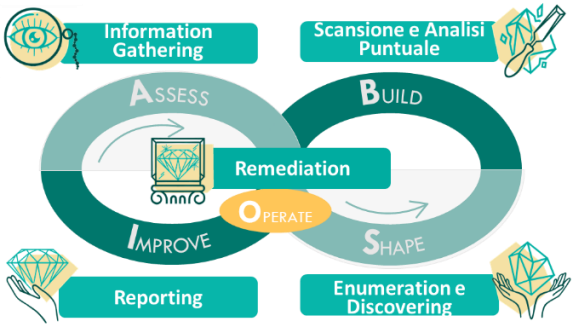
Disponiamo di **Modelli di gestione della sicurezza** già predefiniti per comparto delle PA con evidenza degli elementi rilevanti. Di seguito un esempio:

Caratteristiche comparto	Modello di Analisi dei Fabbisogni di Beni e Servizi – Driver di valutazione
Enti di grande dimensione (es. Ministeri) con estese infrastrutture IT e basi dati, Aziende in-house	► **Modello di Gestione della Sicurezza** completo ed articolato come da Security Framework. ► **Massima flessibilità** per assicurare continuità rispetto ai modelli esistenti se presenti. ► Modellazione di dettaglio dipendente del maggiore o minore grado di esternalizzazione dei servizi IT (es in Cloud – definizione di meccanismi di Cloud Security Governance) ► Ogni elemento può risultare critico. ► Non possono essere predefinite priorità di fabbisogno di acquisto in beni e servizi senza una approfondita situational awareness
Infrastrutture critiche: Operatori Servizi Essenziali (OSE), Perimetro di Sicurezza Nazionale Cibernetica (PSNC)	► **Modello di Gestione della Sicurezza** completo ed articolato come da Security Framework. ► **Disponibilità di template e modelli coerenti agli obblighi di reporting** (assessment e analisi dei rischi basati su CSF nazionale; ruoli necessari, canali di comunicazione verso le autorità preposte) ► In **caso di Operational Technology**, il modello prevede l'introduzione delle specifiche competenze necessarie, nonché l'opportuna estensione dell'anagrafica di **minacce** e vulnerabilità
Strutture sanitarie	► **Modello di Gestione della Sicurezza** commisurato alla missione della struttura: In caso di OSE - si veda modello infrastruttura OSE; In caso di strutture di ricerca - personalizzazione sotto-domini con livelli di maturità target meno stringenti (Security Target Profile) ► Focus sulla sicurezza dei sistemi nel perimetro dell'Ingegneria Clinica (nuovo sotto-dominio). ► Integrazione del Piano sicurezza con quello della struttura Sistemi Informativi
Enti di minori dimensioni e complessità	► Modello di Gestione della Sicurezza semplificato, ► Forte **focalizzazione sulla sensibilizzazione** in materia cyber e digitalizzazione e sulla crescita della cultura del rischio. ► In funzione della strategicità dei servizi e/o della criticità delle basi dati, il modello attinge dai modelli precedenti

5 Proposta progettuale per il servizio "Vulnerability Assessment"

"Se pensi che la tecnologia possa risolvere i tuoi problemi di sicurezza, non capisci i problemi e non capisci la tecnologia" (Bruce Schneier)

Obiettivi del servizio: La complessità e varietà tecnologica e applicativa, in genere riscontrabile presso le PA, determina uno scenario di rischio complessivo elevato, aggravato dalla crescente obsolescenza dei domini tecnologici rispetto al panorama delle minacce informatiche in costante evoluzione. In questo contesto i Servizi di Vulnerability Assessment forniti dal RTI hanno l'obiettivo di **valutare lo stato di esposizione alle vulnerabilità** quali ad esempio configurazioni di sicurezza errate, carenze sui livelli di protezione attivi, applicazioni web e serventi che espongano il contesto ad attacchi interni ed esterni, particolarmente utile in fase di definizione della strategia.



Metodologia: La nostra proposta progettuale valorizza la coerenza sia con i requisiti normativi del GDPR sia con le indicazioni delle Linee guida "Sviluppo software sicuro" AGID (https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro) ed è conforme all'**Open Source Security Testing Methodology Manual** (OSSTMM) di ISECOM ed a quanto definito dalla **Open Web Application Security Project** (OWASP) in tema di security assessment. Le risorse del RTI oltre a essere state parte attiva nella definizione delle suddette linee guida, si avvalgono di una consolidata metodologia, di strumenti leader di settore e acceleratori sviluppati ad-hoc (es. tool e script proprietari) per un aumento della qualità complessiva dei servizi erogati. La metodologia descritta nel corso del paragrafo prevede l'impiego di metodi operativi e strumenti specifici (automatizzati e non intrusivi) che assicurano la raccolta delle vulnerabilità adattandosi alle singole componenti presenti all'interno delle Amministrazioni: infrastrutture IT, IOT/Operational Technology/SCADA e applicative. L'utilizzo di una o più tecniche/strumenti è funzionale all'oggetto di analisi e alle diverse specificità tecnico/organizzative della PA. Le analisi del servizio, così come per i servizi di "Penetration test" e "Testing del codice", saranno contestualizzate nel perimetro e nell'ambiente di riferimento. La validità dei risultati si riferisce al momento in cui gli stessi vengono prodotti ed ai target oggetto di test.

Metodi operativi adottati: Di seguito sono riportati i principali metodi operativi che adotteremo nel corso della fornitura: Frictionless Assessment, Web App Scanning, Agent Assessment, Image Assessment, Passive Assessment, Passive Monitoring, Active Assessment, Active Query.

Strumenti a supporto: Comodo cWatch Vulnerability Scanner Nexpose Community, Tripwire IP360, OpenVAS, Nikto, Wireshark, Aircrack, Nessus Professional, Retina CS Community, Microsoft Baseline Security Analyzer (MBSA). Data la vastità del perimetro di un VA e la sua eterogeneità oltre a quelli indicati utilizzeremo ulteriori 25 strumenti che saranno selezionati in base alle specificità e senza oneri per l'Amministrazione.

5.1 Modalità di esecuzione del servizio

Per massimizzare efficacia e sostenibilità del VA, occorre **ridurre al minimo l'impatto sull'operatività** dei servizi, **utilizzare metriche standard** di valutazione, **configurare i tools** in base al contesto di analisi e **produrre deliverable** che esprimano in modo chiaro e completo tutte le informazioni utili per intraprendere eventuali azioni di mitigation o remediation. In base a quanto descritto, per tutte le attività di testing **si prevede l'utilizzo di un approccio di tipo "Safe Check"**: per ogni vulnerabilità testata gli schemi di attacco non vengono effettivamente portati a termine (tramite exploit o tentativi di ricreare direttamente l'attacco) in quanto le relative operazioni sono interrotte nell'istante che precede l'attacco vero e proprio. Questo metodo permette di evitare interruzioni dei servizi analizzati, nonché il verificarsi di situazioni che potrebbero danneggiare l'Amministrazione.

L'efficacia dell'approccio è assicurato inoltre: ► *dall'utilizzo di opportuni indicatori di rischio* calcolati secondo il framework **Common Vulnerability Scoring System - CVSS** di FIRST (Forum of Incident Response and Security Teams) le cui linee guida sono consultabili all'URL https://www.first.org/cvss e secondo il NVD del NIST (https://nvd.nist.gov/) ► *dall'utilizzo dei codici CVE nella descrizione delle vulnerabilità*. Il **Common Vulnerabilities and Exposures - CVE** rappresenta un dizionario di vulnerabilità e falle di sicurezza, note pubblicamente, le cui linee guida sono consultabili all'URL https://cve.mitre.org/, mantenuto dalla MITRE Corporation. Tale approccio di tipo *risk-based* viene affiancato da un approccio **policy-based**, che prevede la definizione di policy specifiche per il contesto tecnologico dell'Amministrazione e del relativo risk profile. Tali policy vengono utilizzate dagli strumenti citati in precedenza per **prioritizzare automaticamente le vulnerabilità** individuate e assegnarne le relative severità. L'efficacia del processo è assicurata dalla presenza di risorse professionali specializzate dedicate alla supervisione di ogni passo **integrando e perfezionando** quando necessario i risultati degli strumenti automatizzati. Di seguito la descrizione dell'approccio operativo proposto con particolare evidenza dei **risultati attesi** a fronte delle fasi di analisi, esecuzione e assegnazione automatica delle priorità/severità ai rischi di sicurezza:

Assess **Information Gathering:** Vengono raccolte le informazioni per **dettagliare la composizione dell'ecosistema IT** in essere analizzando ed indicizzando le informazioni rilevanti sia attraverso richieste ed operazioni svolte sui sistemi target che tramite interviste con i referenti IT dell'Amministrazione (es. CISO) **(Risultato A) ed il supporto dei Focal Point di Tematica e di Tecnologia** *(cfr. § 3 Struttura Organizzativa)*. In particolare, si effettuerà: ► **Condivisione ed approvazione del piano di test con l'Amministrazione**, contestuale al di kick-off avvio lavori, prevede la stesura di un piano operativo necessario a pianificare e organizzare in modo efficace l'effort delle figure coinvolte lato Amministrazione. Verrà inoltre condiviso il team di figure professionali del RTI a supporto delle attività (es. Security Principal, Penetration Tester Senior/Junior); ► **Raccolta delle**

informazioni relative alla configurazione dell'infrastruttura finalizzata, con il supporto dell'Amministrazione, a individuare i componenti infrastrutturali e/o applicativi oggetto delle attività di analisi, valutando al contempo le opportune fasce orarie di scansione al fine di tutelare l'Amministrazione da qualsiasi fermo.

Shape **Enumeration & Discovering:** Sulla base delle molteplici esperienze maturate, anche in contesti diversi dalla PA quali Financial Service, Manufacturing, Energy, Utilities, ed in coerenza con gli standard internazionali **OWASP e OSSTMM,** il team effettua le seguenti attività: → **Analisi sull'infrastruttura sistemistica o applicativa** oggetto delle attività, al fine di rilevare tutti i sistemi disponibili e i relativi servizi in esecuzione su di essi (discovering) **(Risultato B)**; ► **Creazione di un archivio di target** utile all'Amministrazione come mappa informativa aggiornata **(Risultato C)**. Su ognuno dei sistemi disponibili viene inoltre eseguita un'ulteriore scansione a al fine di rilevare i servizi in esecuzione facendo attenzione a includere i servizi "mascherati" o "nascosti", il relativo versioning e i possibili **punti di criticità (Risultato D)**.

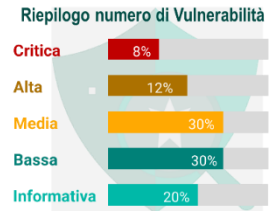
Build **Scansione:** i risultati ottenuti dalle fasi precedenti costituiscono un input per l'adeguata configurazione dei tool di scansione per la ricerca di vulnerabilità, al fine di poter reperire quante più informazioni possibili limitando al minimo il numero di **falsi positivi**. **L'attività di scansione viene condotta in due modalità** sulla base del livello di informazioni/dati inserite in input ai sistemi nel processo di scansione**:** ► **Black-box** senza ausilio di credenziali e ► **Grey/White-box** con tale ausilio. Le scansioni forniscono un primo livello di analisi poi consolidato in un report che, per ciascuna vulnerabilità rilevata, fornisce **informazioni sul target, CVE di riferimento, livello di criticità rispetto alla CVE, PoC**. **(Risultato E)**.

Build **Analisi puntuale: In base alle evidenze** emerse durante gli step precedenti, viene effettuata l'**Analisi delle sezioni critiche o di interesse** valutando l'eventuale livello di rischio **(Risultato F)**. Sulla base della nostra esperienza le vulnerabilità segnalate dalle scansioni automatiche degli strumenti comprendono spesso errori logici che possono non rappresentare un problema di sicurezza a livello di configurazione ma, se sfruttate da un'entità malevola, possono portare ad una violazione di confidenzialità, integrità o disponibilità dei dati, dei servizi o dell'intera infrastruttura.

Efficacia e concretezza delle modalità di esecuzione: Le attività descritte permettono l'acquisizione di risultati caratterizzate da: **Concretezza:** *l'approccio policy-based* descritto, frutto di anni di esperienza maturata in contesti operativi analoghi, garantisce alla PA di identificare lo stato di esposizione ai rischi cyber fornendo un quadro completo delle vulnerabilità rilevate su ogni singola componente dell'infrastruttura. **Efficacia**: *la corretta definizione dei perimetri operativi*, concordati con l'Amministrazione, assicura una gestione ottimale delle risorse a disposizione con una conseguente riduzione dell'effort. L'applicazione delle **linee guida e best practice** del settore viene effettuata tenendo in considerazione vincoli e necessità funzionali dei servizi erogati, delle applicazioni, dell'architettura e delle singole componenti tecnologiche presenti all'interno dell'Amministrazione. L'utilizzo di figure professionali altamente specializzate (*cfr § 16 Aggiornamento delle risorse professionali*), permette di affinare ulteriormente **l'analisi automatica prodotta dagli strumenti software** (assegnazione automatica delle priorità e severità ai rischi di sicurezza), validandone i risultati in funzione del contesto di rischio.

5.2 Proposta di elaborazione di un "Remediation plan" e Reportistica di sintesi

Improve **Reporting:** Durante le attività di "Reporting" vengono raccolti e classificati tutti i problemi di sicurezza rilevati al fine di fornire una visione dettagliata degli obiettivi, dei metodi e dei risultati prodotti e descritti in precedenza. In tale fase viene fatta sintesi delle evidenze emerse riclassificando le vulnerabilità in base alle severity definite all'interno dello standard **Common Vulnerability Scoring System (CVSS)** e associandogli un livello di priorità adeguato in funzione del contesto di esposizione della vulnerabilità stessa. In questo modo verrà assegnato un valore numerico ed oggettivo alla gravità delle vulnerabilità, permettendo di dare priorità alle azioni di remediation. Nella redazione dei report viene utilizzata la lista redatta dall'**OWASP 2021 Top 10** e la lista **OWASP 2016 Mobile Top 10** selezionati dal RTI per l'efficacia della assegnazione di rischio concentrata sulle vulnerabilità più rilevanti all'interno del singolo scenario tecnologico.



Il report di sintesi conclusivo è strutturato con informazioni di carattere qualitativo e quantitativo: ► **Scope:** fascia temporale in cui è stata eseguita l'attività di VA e per completezza vengono indicati i dettagli e le informazioni dei target oggetto delle analisi. L'indicazione temporale è elemento fondamentale in quanto consente di escludere, nelle successive fasi di analisi, eventuali correlazioni fra le attività degli analisti ed eventi eccezionali legati alla normale operatività dei sistemi. ► **Tools:** descrizione degli strumenti e tecniche utilizzate. ► **Executive Summary:** overview ad alto livello delle vulnerabilità, pensata per essere indirizzata ai diversi stakelholder dell'Amministrazione, con opportune raccomandazioni per l'implementazione di remediation o di fix immediate in caso di vulnerabilità di severity "high" o "critical" e a seconda che il target sia già stato rilasciato o meno in ambiente di produzione. ► **Technical Details** contenente i dettagli tecnici dell'attività con le evidenze riscontrate, corredata da una parte descrittiva delle vulnerabilità individuate e i potenziali impatti su risorse, infrastruttura, sistemi, processi, sistemi applicativi e aree di business dell'Amministrazione. Le vulnerabilità sono rappresentate in forma tabellare, fornendo per ognuna di esse le seguenti informazioni: **nome, categoria OWASP Top Ten, "Vector String"** (il modo in cui viene assegnata la severity alla vulnerabilità) e infine il **CVSS Base Score** (punteggio calcolato in base alla severity della vulnerabilità).

Operate **Remediation:** I risultati fin qui esposti consentono all'Amministrazione di acquisire piena consapevolezza sullo stato di esposizione alle vulnerabilità mediante raccolta di informazioni su servizi erogati, applicazioni, architettura e componenti tecnologiche. Il Remediation plan, documento di dettaglio personalizzato che riporta tutte le criticità individuate nelle fasi precedenti, fornisce una completa e chiara descrizione di tutte le attività legate ad uno specifico piano di rientro e necessarie per una corretta riduzione del

rischio cyber. L'approccio per la stesura di tale documento è ancora una volta di tipo *risk based*, che **considera le vulnerabilità in base alla potenziale superficie di attacco**, fornendo così una **priorità** ai singoli livelli di rischio in funzione delle necessità di business della singola Amministrazione. Nell'identificazione delle attività viene presa in considerazione la *sostenibilità dei singoli interventi* sia da un punto di vista economico che tecnologico, e la possibilità di efficientare i diversi interventi verificando ad esempio l'eventuale concorrenza di più vulnerabilità su di un singolo asset o parte di sistema. Le indicazioni operative per le singole attività di remediation prenderanno in considerazione eventuali *standard operativi* già in essere all'interno dell'Amministrazione, contribuendo all'ottimizzazione dell'intero processo.

Il remediation plan, personalizzato sulla singola Amministrazione, conterrà elementi qualitativi e quantitativi/dimensionali: ► **la descrizione della problematica rilevata**. La metodologia messa in atto dal Team descriverà e dettaglierà tutte le problematiche individuate con le relative informazioni. Oggetto della valutazione sarà l'impatto e valutazione qualitativa del rischio. La misurazione dei singoli eventi rischiosi consentirà di distribuirli secondo la loro criticità e di selezionare quelli su cui intervenire. ► **l'indicazione della root-cause.** L'obiettivo principale è fornire all'Amministrazione un chiaro livello di approfondimento sulle conseguenze che potrebbero scatenarsi in seguito ad uno specifico evento e che cosa si può/deve fare per evitare che possa accadere. La priorità degli eventi da analizzare è generalmente definita in base alla gravità dell'evento e al livello di rischio potenziale. ► **la descrizione delle attività da porre in essere per risolvere la problematica.** Consiste negli step di definizione delle azioni intraprendere affinché vengano effettuate le modifiche richieste a risolvere la problematica. Una stima qualitativa (alto, medio, basso, sulla base di criteri concordati con il referente dell'Amministrazione) dell'impatto economico, organizzativo e tecnologico dell'intervento. ► **una stima temporale dell'intervento.** Un'attenta proposta di elaborazione di remediation plan non può assolutamente precludere un attento studio temporale dell'intervento. Il nostro team di analisti si affiancherà all'Amministrazione nel comprendere eventuali esigenze operative, con l'obiettivo disegnare al meglio tutte le singole fasi in orari sostenibili per le attività di business al fine di ridurre gli impatti. ► **la priorità di implementazione dell'intervento**. permetterà al cliente di prendere contezza di come andranno pianificate e distribuite le modifiche sui target impattati (infrastrutturali o applicativi), corretta pianificazione e riavvio dei servizi e sistemi, eventuale valutazione nell'applicabilità di script o GPO policy per l'automazione del deploy, ed infine pianificazione della correzione di codice non sicuro (bugfix).

Le fasi di reporting e remediation fin qui descritte si distinguono per concretezza ed efficacia in quanto viene *prodotto un documento esaustivo* contenente il dettaglio delle singole vulnerabilità, le relative root-cause, il grado di severity e di priority, ed un remediation plan in grado *di indicare all'Amministrazione tutte quelle azioni che devono essere impiegate*, in termini di risorse economiche e/o tecniche funzionali, per una corretta risoluzione.

6 Proposta progettuale per il servizio "Testing Del Codice"

"Il test di un programma può essere usato per mostrare la presenza di bug, ma mai per mostrare la sua assenza"
(Edsger Wybe Dijkstra)

Obiettivi del servizio: indirizzare la produzione di applicazioni sicure ed efficienti minimizzando gli impatti operativi e l'effort dell'Amministrazione, grazie al supporto di professionisti altamente specializzati e all'adozione di strumenti in grado di automatizzare sia il testing del codice (statico e dinamico) che la produzione delle schede tecniche di dettaglio utili alla produzione dei report (technical e executive) elaborate dai Security Analyst.

Metodologia: L'approccio metodologico adottato dal RTI per il servizio di Testing del Codice si basa **sul framework DevSecOps curato dal Centro di Competenza di Application Security** ed è integrabile nel **Software Development Life Cycle (SDLC) d**ell'Amministrazione.

Standard adottati: Gli standard indicati sono stati individuati dal RTI sulla base di conoscenze approfondite dell'Information Security di riferimento quali ad esempio **AgID** (Linee guida per lo sviluppo sicuro del codice), **OWASP** (OWASP Software Assurance Maturity Model, OWASP Development Guide, OWASP Testing Guide, OWASP Cheat Sheets, OWASP Secure Coding Practices), **SAFECode** (Software Assurance Forum for Excellence in Code)**, WASC** (Web Application Security Consortium)**, CAPEC** (CERT Secure Coding e Common Attack Pattern Enumeration and Classification)**, OSSTMM** (Open Source Security Testing Methodology Manual).

In coerenza con l'approccio Idea, di seguito la metodologia adottata:

Assess **Definizione:** definizione della **mappa applicativa**, comprensione della **matrice di valutazione dei rischi** e della superficie d'attacco, indispensabile per definire la lista degli interventi dell'Amministrazione contraente (anche rispetto al SLDC adottato);

Shape **Prioritizzazione:** in relazione alla mappa applicativa e alla matrice dei rischi, definizione delle **priorità di intervento** (per aree, sistemi e applicativi) con valutazione specifica rispetto alle caratteristiche dell'Amministrazione contraente almeno rispetto a: processi, risorse e strumenti adottati per la gestione del SLDC;

Build **Configurazione:** in relazione alle priorità di intervento identificate nella fase precedente sono eseguite le attività di: **ridisegno del processo di SDLC** adottato dall'Amministrazione, la **configurazioni degli strumenti** messi a disposizione dal RTI (utili al testing del codice e al reporting ed integrati con il processo formalizzato) e l'**affiancamento delle risorse** dell'Amministrazione identificate al fine di garantire la corretta adozione di processi/strumenti e supportare l'Amministrazione nella corretta interpretazione

dell'executive report (vista di sintesi) e del techincal report (elenco delle vulnerabilità indentificate con relativa sezioni di codice) redatto dai Security Analyst sulla base delle evidenze prodotte dai vari tool configurati;

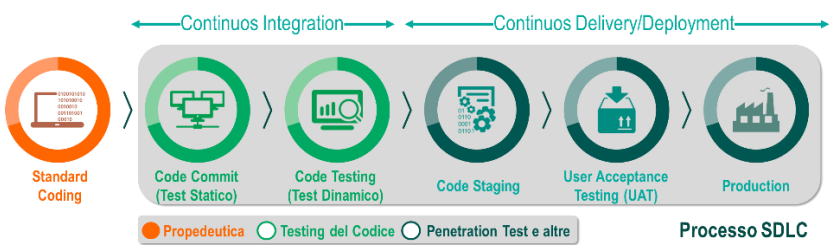
Remediation Plan: in relazione alle evidenze emerse viene formalizzato un **piano di miglioramento continuo** indispensabile per identificare e prioritizzare eventuali interventi su: processo SDLC (miglioramento del processo adottato), strumenti (attività di fine tuning sulle configurazioni eseguite) e risorse (attività di formazione e training-on-the-job). Verrà inoltre formalizzato un **remediation plan** sugli applicativi esaminati rispetto alle evidenze emerse dal technical report secondo un *approccio risk-based*.

Continuos Improvement: supporto continuativo all'Amministrazione contraente al fine di garantire il **miglioramento continuo** del processo di SDLC definito, degli strumenti adottati (configurati e integrati all'interno delle piattaforme di release e build management) oltre che del training-on-the-job offerto alle risorse dell'Amministrazione.

Strumenti a supporto: gli strumenti messi a disposizione dal RTI (Jenkins, Junit, SonarQube, Coverty, Fortify, Burp, Ghidra, JD-GUI, Frida, iNalyzer) permettono l'integrazione del framework DevSecOps all'interno del SDLC (*crf. § 6.3 Strumenti adottati e Integrazione per il Testing del Codice*)

6.1 Modalità di esecuzione del servizio

Descriviamo nel dettaglio le attività di testing del codice (statico, dinamico e mobile) rispetto alla catena di Continuous Integration e Continuous Delivery (CI/CD) schematizzata, coerente con lo standard DevSecOps proposto dal RTI



Attività/Servizio	Analisi Statica	Analisi Dinamica	Analisi Mobile
Standard & Plan	✓	✓	✓
Code Commit	✓	✗	✓
Code Testing	✗	✓	✓

Come riportato in figura i servizi di Testing del Codice si posizionano all'interno delle attività di "Standard&Plan", "Code Commit" e "Code Testing" della fase di Continuous Integration, garantendo la *completa efficacia e concretezza* rispetto alle modalità di esecuzione del servizio di seguito descritto.

6.1.1 Analisi Statica

Il servizio di Testing del Codice che intendiamo implementare per l'Analisi Statica è orientato **all'identificazione di vulnerabilità software presenti all'interno del codice, comprensivo della valutazione di librerie terze utilizzate, a *"commit-time"*,** ovvero ogni volta che viene eseguita l'archiviazione del codice sorgente sul repository software centrale dell'Amministrazione, grazie all'integrazione degli **strumenti di CI/CD**. Queste le fasi operative previste:

Standard & Plan: l'attività ha come obiettivo quello di **formalizzare gli standard di riferimento** (sia in termini di sicurezza che coding) da adottare per lo sviluppo e definire le logiche/regole di integrazione con i repository dell'Amministrazione indispensabili per lo scambio del codice sorgente (es. File Transfer Service proprietario del RTI oppure tramite integrazione con strumenti di code management dell'Amministrazione come SVN, CVS, Git o TFVC qualora non si decida di intervenire direttamente sugli ambienti di Build&Release Management dell'Amministrazione). In particolare, i test di sicurezza minimi che verranno eseguiti agiranno su aspetti semantici e sintattici rispetto a: service exposure, data validation, third-party library, control flow e buffer validation e faranno riferimento al documento di Best Practice e Linee Guida messo a disposizione dell'Amministrazione da parte del RTI.

Code Commit: ogni qual volta che verrà archiviato il codice sorgente all'interno del repository dell'Amministrazione (o all'interno dell'area di interscambio del codice sorgente tra Amministrazione e RTI), verranno avviati i test di sicurezza definiti durante l'attività precedente che andranno ad analizzare oltre che il codice sorgente prodotto tutte le librerie e servizi di terze parti utilizzate. Tale attività oltre a poter essere configurata attraverso gli strumenti di **Continuous Integration Server** messi a disposizione dal RTI *(crf § 6.3 Strumenti adottati e Integrazione per il Testing del Codice*) potrà essere schedulata manualmente ogni qual volta lo si riterrà opportuno. Per ogni vulnerabilità identificata verrà prodotta una **scheda tecnica** di dettaglio con le seguenti informazioni: ► **ID** (identificativo progressivo della issue rilevata costruita secondo la seguente sintassi <APPLIVATIVO><DATA><BUILDVERSION><PROGESSIVO>), ► **Tipologia** (riferimento specifico alla best-practice/linea guida violata) , ► **Descrizione** (descrizione sintetica dell'issue rilevata come da standard e linee guida), ► **Evidenza** (identificazione della sezione esatta di codice sorgente compresi eventuali file di configurazione) e ► **Severità** (valutazione della severità della violazione in termini di sicurezza come da standard adottati). Tali schede di dettaglio sono gestite direttamente dal Continuous Integration Server, messe in relazione ad una specifica build dell'applicativo in esame, e rese disponibili nel Portale di Fornitura per la consultazione on/off-line del team di lavoro che le utilizzerà per produrre sia il **Technical** che **l'Executive Report**.

Reporting (Technical & Executive): a partire dalle evidenze prodotte nella fase precedente i Security Analyst analizzeranno le informazioni riportate all'interno delle schede tecniche al fine di elaborare un report di dettaglio che oltre a considerare il livello di severità identificato valuta gli elementi di contesto riportati all'interno dei documenti di Mappa Applicativa e di Matrice dei Rischi prodotti entrambi nella fase di Assess. Più nello specifico il **Technical Report** arricchirà ogni scheda tecnica con le informazioni di: ► **Priorità di Risoluzione** (assegnazione di una priorità secondo la scala alta/media/bassa in relazione al rischio correlato valutato rispetto ad elementi come: sicurezza perimetrale, esposizione dei servizi su rete interna o esterna, tipologia accessi e frequenza, tipologia di informazioni conservate, livello di integrazione/isolamento, ecc.), ► **Difficoltà di Risoluzione** (valutazione dell'effort necessario per eseguire la patch di sicurezza secondo la scala alta/media/rapida) ► **Mitigazione** (azione correttiva su codice sorgente e/o file di configurazione da

apportare al fine di garantire il rientro l'issue di sicurezza). Per quanto concerne l'**Executive Report** i Security Analyst (a partire dal Technical Report) elaboreranno una vista di sintesi sia di tipo tabellare che grafica (in riferimento a quanto già riportato nella mappa applicativa) al fine di verificare e valutare opportunatamente eventuali rischi correlati. Tutte le informazioni elaborate sia a livello di Technical Report che Executive Report potranno essere consultate sia in modalità off-line (es. PDF/DOCS File) che on-line direttamente all'interno del Portale della Fornitura.

6.1.2 Analisi Dinamica

Il servizio di Testing del Codice che intendiamo implementare per l'Analisi Dinamica è orientato all'**identificazione delle vulnerabilità software presenti all'interno del codice binario/compilato degli applicativi**. L'analisi verrà condotta a *"compile-time"* (ossia ogni volta che viene eseguita la compilazione e il packaging del codice sorgente conservato all'interno del repository software centrale) grazie all'integrazione degli strumenti di CI/CD. Il servizio di analisi dinamica del codice sorgente sarà condotto attraverso le attività riportate nel seguito del paragrafo.

Standard & Plan: l'attività oltre a fare riferimento a quanto già descritto nel paragrafo relativo all'analisi statica del codice definisce la modalità di esecuzione dei test dinamici. In particolare, sarà possibile adottare un approccio di tipo **Stage&Gate** (test dinamici eseguiti a valle dei test statici e solo nel caso in cui siano garantiti i requisiti minimi di sicurezza) o **Passthrough** (test dinamici eseguiti direttamente a partire dal codice binario/compilato). In entrambi i casi i test di sicurezza dinamici minimi che verranno eseguiti verificheranno aspetti di: autenticazione, gestione della sessione, controllo degli accessi, validazione (e cifratura dei) dati, configurazione, audit, logging e error handling e faranno riferimento ad un documento di Best Practice e Linee Guida messo a disposizione dell'Amministrazione da parte dell'RTI e sulla base del quale verranno eseguiti i test del codice. A titolo esemplificativo e non esaustivo subito sotto sono riportati alcune pagine del documento.

ID Requisito	AUT-001
Descrizione	Le credenziali o in generale le informazioni sensibili che vengono scambiate tra client e server (quali cookie di autenticazione), oppure tra i vari livelli di un'applicazione web, dovrebbero sempre transitare su canale criptato. Assicurarsi che per le informazioni sensibili o riservate (come ad esempio username o password) sia implementato un canale cifrato (HTTPS) per l'invio delle informazioni. Utilizzare solo il metodo POST HTTP per l'invio delle credenziali.
Java/J2ee/Tomcat	Aggiungere nel file di configurazione web.xml il seguente codice: <security-constraint> <web-resource-collection> <web-resource-name>Security page </web-resource-name> <url-pattern>/web/login/signup.jsp</url-pattern> </web-resource-collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</transport-guarantee> </user-data-constraint> </security-constraint>
Riferimento per verifica	OWASP-AT-001 http://www.owasp.org/index.php/Testing_for_credentials_transport_(OWASP-AT-001)

ID Requisito	CM-001
Descrizione	È necessario non esporre le console di management dell'applicazione, o in generale di permetterne l'accesso solo ad utenti locali (Intranet). L'accesso può quindi essere effettuato internamente attraverso un tunnel SSH o tramite VPN dall'esterno. Assicurarsi che non vi siano credenziali di default e che siano implementate password policy robuste. Tale requisito va applicato anche a tutte le console di management di Jboss ove utilizzato.
Java/J2ee/Tomcat	Modificare il file web.xml principale dell'applicazione di amministrazione con i seguenti valori: <security-constraint> <web-resource-collection> <url-pattern>/*</url-pattern> </web-resource-collection> <auth-constraint> <role-name>admin</role-name> </auth-constraint> </security-constraint> Si raccomanda, inoltre di non inserire nessuno specifico http-method nella restrizione di accesso, dal momento che apre potenzialmente l'accesso attraverso alcune modalità di attacco.
Riferimento per verifica	OWASP-CM-007 http://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)

ID Requisito	SM-005
Descrizione	Per le applicazioni critiche, implementare un controllo che verifichi che un utente già autenticato non possa aprire una nuova sessione fino allo scadere della sessione attiva. Nel caso in cui si verifichi tale situazione, segnalare e tenere traccia dell'evento. Assicurarsi inoltre che l'IP dell'utente sia legato alla sua sessione quando l'utente accede alle risorse dell'applicazione.

Java/J2ee/struts	Aggiungere l'IP di provenienza in sessione all'atto del login.
	request.getSession().setAttribute("IP",request.getRemoteAddr());
	successivamente inserire in un filtro di controllo il check dell'IP da cui è generata la richiesta con quello in sessione.
	public void doFilter(ServletRequest req, ServletResponse res,
	FilterChain chain).{
	If(req.getSession()!=null &&
	!req.getSession().getAttribute("IP").equals(req.getRemoteAddr()))
	// potential session hijacking, throw loginException
	else
	// go on with filtering
	}

Riferimento per verifica	OWASP-SM-001 http://www.owasp.org/index.php/Testing_for_Session_Management_Schema_(OWASP-SM-001)

Code Testing: in relazione al tipo di approccio adottato (Stage&Gate Vs Passthrough) e ogni qual volta che verrà eseguito il packaging dell'applicativo a partire dal repository dell'Amministrazione (o depositato il file binario/compilato dell'area di interscambio tra Amministrazione e RTI) verranno avviati i test di sicurezza dinamici. Tale attività oltre a poter essere configurata attraverso lo strumento di **Continuous Integration Server messo a disposizione dal RTI** (*cfr. § 6.3 Strumenti adottati e Integrazione per il Testing del Codice*) potrà essere schedulata manualmente ogni qual volta lo si riterrà opportuno. I test guidati dal team mirano a verificare comportamenti del sistema anomali o potenziali vulnerabilità e si concentreranno sulla **superficie esposta di una applicazione up-&-running** testandone il comportamento dinamico rispetto ad una sollecitazione esterna malevola. Ciò richiede la predisposizione di **staging areas** (gestite anche direttamente dagli strumenti di Continuous Integration) all'interno delle quali predisporre un ambiente sicuro e controllato ove eseguire i test preventivati attraverso degli strumenti descritti nel seguito del documento. Analogamente a quanto già descritto nel caso di analisi statica del codice per ogni vulnerabilità identificata verrà prodotta una **scheda tecnica** di dettaglio secondo le modalità ed il tracciato già descritte in precedenza con l'aggiunta dell'informazione relativa al **Digest** (identificativo del codice/package binario analizzato).

Reporting (Technical & Executive): a partire dalle evidenze prodotte a "compile-time" il Team analizzerà le informazioni riportate all'interno delle schede tecniche al fine di elaborare un report di dettaglio che oltre a considerare il livello di severità identificato valuti gli elementi di contesto sintetizzati all'interno del documenti di Mappa Applicativa e di Matrice dei Rischi prodotti entrambi nella fase di Assess analogamente a quanto già descritto nell'ambito dell'ambito dell'analisi statice del codice.

6.1.3 Mobile

Il servizio di Testing del Codice che intendiamo implementare per l'Analisi delle Applicazioni Mobile è orientato all'identificazione delle vulnerabilità del software sia a livello di codice sorgente che a livello di codice binario/compilato. L'analisi verrà **condotta seguendo quanto già presentato per l'analisi Statica e Dinamica del codice** seguendo la logica di servizio a canone annuo (rispetto le fasce 1,2 e 3 del Capitolato Tecnico).

Standard & Plan: La modalità di esecuzione per le Applicazioni Mobile (iOS, Android e Windows Phone) sarà solo di tipo **Stage&Gate** (test dinamici eseguiti a valle dei test statici e solo nel caso in cui siano garantiti i requisiti minimi di sicurezza) e punterà a rilevare le vulnerabilità già presentate in precedenza con particolare enfasi alla verifica delle policy adottate per gestire gli accessi ai dati e alle funzioni del dispositivo.

Code Commit: ogni qual volta che verrà eseguito un commit all'interno del repository dell'Amministrazione (o all'interno dell'area di interscambio del codice sorgente tra Amministrazione e RTI), verranno avviati i test di sicurezza definiti durante l'attività precedente che andranno ad analizzare oltre che il

codice sorgente prodotto tutte le librerie e servizi di terze parti utilizzate (modalità scansioni periodiche). L'analisi statica del codice sorgente Java/Swift avverà usando software di settore quali XCode (Ghidra) nativo per iOS o Lint nativo di Android (JD-Gui) con gli obiettivi e tecniche di analisi citati all'inizio del paragrafo per l'analisi statica del codice ma usando una base di conoscenza di regex uniche per l'ambiente Mobile, in compliance alla OWASP Top 10 Mobile, OSSTMM ed altri standard di settore.

Code Testing: ogni qual volta che verrà eseguito il packaging dell'applicativo a partire dal repository dell'Amministrazione (o depositato all'interno di APP market place "interni") verranno avviati i test di sicurezza dinamici (modalità scansioni periodiche). L'analisi dinamica dell'APP avverrà in sandbox ovvero in ambiente chiuso e controllato facendo leva su strumenti di settore quali Frida, iNalyzer, Charles, al fine di evidenziare eventuali problemi di sicurezza di natura Web, cercando di determinare se l'applicazione in questione comunica con interfacce di altri sistemi e/o applicazioni così come con altre risorse collegate che potrebbero avere un impatto sulla sicurezza globale del sistema, evidenziando eventuali errori logici che potrebbero portare ad una grave violazione di confidenzialità, integrità o disponibilità dei dati, dei servizi o dell'intera infrastruttura.

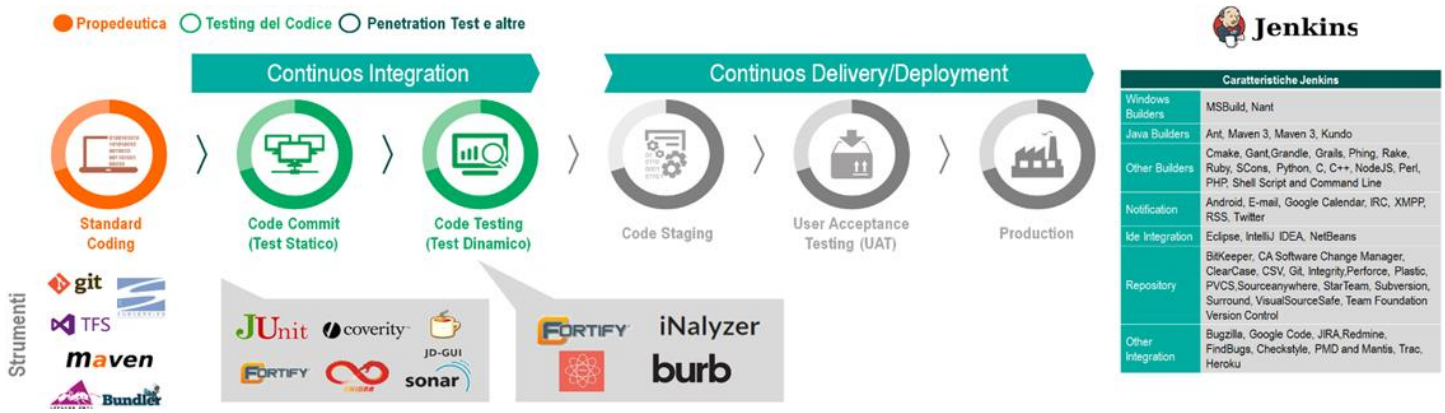
Reporting (Technical & Executive): a partire dalle evidenze prodotte il Team specializzato analizzerà le informazioni riportate all'interno delle schede tecniche al fine di elaborare un report di dettaglio che oltre a considerare il livello di severità identificato valuti gli elementi di contesto sintetizzati all'interno del documenti di Mappa Applicativa e di Matrice dei Rischi prodotti entrambi nella fase di Assess analogamente a quanto già descritto nell'ambito dell'ambito dell'analisi statica del codice.

6.2 Remediation Plan

In relazione ai test sul codice eseguiti (statici, dinamici e mobile) i Security Analyst, elaboreranno il **remediation plan** indispensabile per identificare le attività di bonifica da implementare su ciascuna componente impattata comprensivo della road-map di interventi. L'approccio alla base della stesura di tale documento è di tipo *risk based*, e vengono considerate le vulnerabilità in base alla potenziale superficie di attacco, fornendo così una priorità ai singoli livelli di rischio in funzione delle necessità di business della singola Amministrazione. Nell'identificazione delle attività verrà presa in considerazione la *sostenibilità dei singoli interventi* sia da un punto di vista economico che tecnologico, e la possibilità di efficientare i diversi interventi verificando, ad esempio, l'eventuale concorrenza di più vulnerabilità su di un singolo asset o parte di sistema. Le indicazioni operative per le singole attività di remediation prenderanno in considerazione eventuali standard operativi già in essere all'interno dell'Amministrazione, *contribuendo all'ottimizzazione dell'intero processo*. Il documento in particolare conterrà almeno le sezioni ► **Vulnerability Technical Analysis** dove si classificherà, mediante criteri di violazione agli standard sopra citati, ciascuna vulnerabilità confermata e si darà evidenza della relativa prioritizzazione formulata sulla base della sua intrinseca gravità, della raggiungibilità dell'asset coinvolto, della difficoltà di sfruttamento, della vulnerabilità stessa e di quanto questa sia nota, e dell'impatto in caso di sfruttamento; ► **Vulnerability Remediation** dove creare e condividere con l'Amministrazione criteri di analisi per suggerire in maniera costruttiva, per ciascuna vulnerabilità comunicata nei technical ed executive reports, un piano di bonifica della stessa inclusivo di pre-requisiti necessari all'espletamento dell'attività (es. uso di libreria open-source non presente in perimetro, upgrade della versione del linguaggio di programmazione, ecc.), offrendo continuativo supporto agli stakeholders per la corretta ed esaustiva implementazione di ogni azione di bonifica.

6.3 Strumenti adottati e Integrazione per il Testing del Codice

Come già descritto in precedenza la metodologia adottata dal RTI si basa sul framework DevSecOps che ha come obiettivo quello di semplificare, standardizzare e automatizzare il processo di sviluppo software sia in termini di operations che di developing garantendo un approccio security-by-design e security-by-default attraverso l'adozione di una serie di strumenti di automazione integrati nel SDLC e orchestrati dal Continuous Integration Server. Il RTI nell'ambito della fornitura dei servizi in oggetto, metterà a disposizione dell'Amministrazione il tool Continuous Integration Server (Jenkins) senza alcun onere aggiuntivo per l'Amministrazione che consente piena integrabilità con gli strumenti identificati a capitolato tecnico (SVN - Subversion, CVS - Concurrent Versions System, Git, TFVC - Team Foundation Version Control). Inoltre, oltre ad essere riportate le caratteristiche principali del server di integrazione è rappresentato il SDLC standard proposto dall'RTI (con relativi strumenti messi a disposizione dell'Amministrazione da parte dell'RTI per ogni fase del processo) nel caso in cui si preveda un'integrazione sui sistemi di Code Repository.



7 Proposta progettuale per il servizio "Supporto all'analisi e gestione degli incidenti"

Ci sono solo due tipologie di organizzazione: quelle che sono state hackerate e quelle che lo saranno
(Robert Muller, direttore del FBI)

Obiettivi del servizio: supportare le Amministrazioni nelle fasi di analisi, progettazione e verifica post-mortem dei processi di gestione degli incidenti di sicurezza, nonché nella opportuna condivisione delle informazioni ottenute e delle diagnosi effettuate al fine di minimizzare l'insorgenza di ulteriori incidenti e l'impatto avverso.

Metodologia: il RTI possiede un bagaglio di profonda esperienza di Security Incident Management maturata nel corso di centinaia di progetti, svolti avvalendosi di profonda competenza su best practice e standard nazionali, (es. CERT-Agid) e internazionali, quali la "Computer Security Incident Handling Guide" del NIST. in base alla quale ha potuto sviluppare un **approccio metodologico** ad hoc, illustrato in figura:

Assess **Preparazione:** vengono svolte le attività necessarie a supportare le Amministrazioni nella **definizione, implementazione e miglioramento continuo di un processo** di gestione degli incidenti di sicurezza finalizzato a prevenire, rispondere, limitare gli impatti e apprendere dagli incidenti di sicurezza. Tali attività includono, ad esempio, la creazione e gestione di un piano di risposta agli incidenti (IRP), la definizione delle modalità di classificazione della remediation dell'incidente, delle modalità di analisi dei log e degli eventi, dei processi di analisi post-mortem, dei processi di escalation verso le entità interne ed esterne (inclusi CSIRT-Italia, organi di polizia giudiziaria), delle modalità di gestione delle comunicazioni interne/esterne e degli aggiornamenti, ecc.

Rilevazione e analisi e Contenimento, erogazione e recovery sono attività incluse nell'ambito della fornitura del servizio SOC del Lotto 1 e pertanto qui non trattate.

Improve **Post-incident activities**: vengono svolte le attività finalizzate a **identificare le root-cause dell'incidente e adottare le necessarie azioni a livello tecnologico e / o organizzativo** per prevenire la sua reiterazione in futuro. Tali attività includono tipicamente l'acquisizione, in loco o da remoto, delle evidenze digitali afferenti all'incidente mediante tecniche di informatica forense, nonché la successiva analisi delle stesse mediante strumenti e tecniche specifiche per il caso di specie (es. log analysis, network forensics, malware forensics, system forensics, ecc.).

Metodi: Di seguito l'elenco dei principali metodi adottati nel corso della fornitura: ► **organizzazione e facilitazione di workshop dedicati** con i referenti chiave dell'Amministrazione al fine di rilevare le *capability* già in essere per la gestione degli incidenti in termini di procedure, prassi operative, competenze, strumenti tecnologici, ecc., nonché a comprendere le necessità e le aspettative per l'intervento in corso; ► **utilizzo di checklist e template per l'Incident Forensics**, realizzate tramite strumenti di office automation, finalizzate a delimitare, tramite compilazione guidata con i referenti tecnici dell'Amministrazione, il perimetro dell'incidente e identificare quindi gli asset oggetto di acquisizione e analisi forense.

Standard adottati: Di seguito l'elenco dei principali standard adottati nel corso della fornitura: ► **ISO/IEC 27035-1:2016 - "Part 1**: Principles of incident management". ► **ISO/IEC 27035-2:2016 - "Part 2**: Guidelines to plan and prepare for incident response". ► **ISO/IEC 27035-3:2020** - "Part 3: Guidelines for ICT incident response operations". ► **ISO/IEC 27037:2012** - "Guidelines for identification, collection, acquisition, and preservation of digital evidence". ► **ISO/IEC 27042:2015** - "Guidelines for the analysis and interpretation of digital evidence". ► **NIST SP 800-61 Rev. 2** - "Computer Security Incident Handling Guide". ► **NIST SP 800-83 Rev. 1** - "Guide to Malware Incident Prevention and Handling for Desktops and Laptops". ► **Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali dell'AGID**. ► **Pubblicazioni e guide di fonti istituzionali** quali CSIRT Italia e CERT-AgID con particolare riferimento alle "linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali" dell'AgID, che forniscono numerosi strumenti utili quali matrici di classificazione e prioritizzazione degli incidenti, tassonomie e workflow dei processi di gestione e comunicazione.

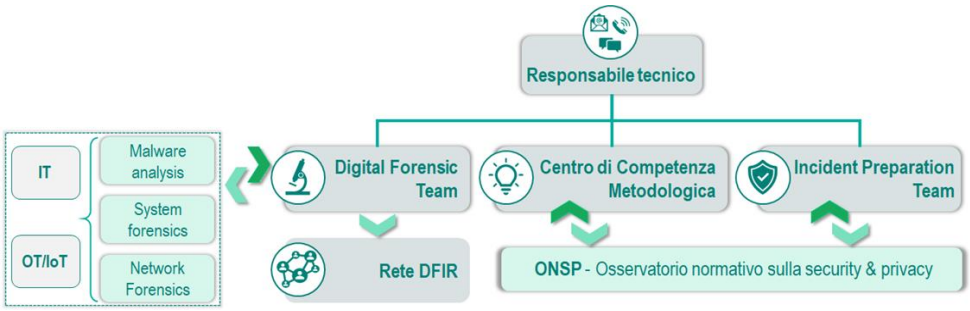
Strumenti a supporto: A supporto delle attività di gestione degli incidenti il Security Principal/Analyst e i Forensic Experts utilizzano i migliori strumenti disponibili sul mercato, siano essi open source o proprietari già acquistati dal RTI, che può quindi metterli a disposizione senza alcun onere per l'Amministrazione. Il RTI dispone inoltre di **acceleratori sviluppati ad-hoc** per un aumento della qualità complessiva dei servizi erogati e il contenimento dei tempi di esecuzione. **Strumenti proposti per le attività di analisi forense:** ► **EnCase, Axiom, X-Ways, Autopsy Digital Forensics**: piattaforme di Digital Forensics, utilizzate sia per l'acquisizione dei dispositivi con tecniche forensi, sia per la loro analisi; ► **UFED**: strumento per eseguire attività di Mobile Forensics, dall'acquisizione del dispositivo sul campo all'analisi dei suoi contenuti sul campo o in laboratorio; ► **CAINE Linux, Ttsurugi Linux, SIFT Workstation**: distribuzioni Linux che possono essere utilizzate sia in modalità "live" per acquisire in modo forense dei sistemi da analizzare, sia come workstation per l'analisi vera e propria degli artefatti acquisiti; ► **Plaso**: strumento utilizzato per generare la cosiddetta super timeline, utile a dettagliare quanti più eventi possibili durante l'analisi di un dispositivo digitale, come il suo traffico Internet, le e-mail ricevute e inviate, le operazioni eseguite dall'utente, ecc.; ► **Timesketch**: piattaforma web per l'analisi collaborativa della super timeline, generata per esempio tramite Plaso; ► **Volatility**: framework utilizzato per l'analisi forense della memoria volatile (es. RAM) dei dispositivi analizzati, tramite il quale si possono ottenere utili informazioni per arricchire la super timeline, o per analizzare un malware che si nasconde in memoria; ► **Velociraptor**: strumento open source utile per il monitoraggio

degli endpoint durante o a seguito di un incidente, ivi inclusa la raccolta degli artefatti dagli stessi per una loro analisi forense. ► gli **strumenti messi a disposizione da fonti istituzionali** quali il CERT-AgID e il CSIRT (es. https://cert-agid.gov.it/strumenti/).

Strumenti proposti a supporto delle attività dell'Incident Preparation Team: ► **Incident Best Practice Repository** documentale, centralizzato a livello di fornitura, utilizzato per la continua alimentazione e condivisione di una knowledge-base sulle *migliori pratiche, casi d'uso reali e success story* relative all'implementazione di processi di gestione degli incidenti di sicurezza in ambito PA, preventivamente anonimizzate con la messa a disposizione delle sole informazioni utili a fornire valore aggiunto in termini di uniformità ed efficacia alle attività progettuali. ► **CSIRT Maturity assessment**, toolkit ENISA - European Union Agency for Cybersecurity, che consente di misurare in maniera efficace, ripetibile e comparabile il livello di maturità di un Computer Security Incident Response Team secondo il modello SIM3 definito dall'Open CSIRT Foundation, nonché ulteriori strumenti messi a disposizione da ENISA come la *good practice guide* "How to setup up CSIRT and SOC"

7.1 Modello organizzativo adottato e strumenti proposti per le attività di analisi forense

Il modello organizzativo prevede i seguenti **organismi e strutture**: ► Un **Responsabile Tecnico**, corrispondente alla figura professionale di *Senior Security Analyst* prevista dalla documentazione di gara, raggiungibile in modalità multicanale (telefono, e-mail, messaggistica istantanea, ecc.), la cui responsabilità principale sarà raccogliere gli elementi preliminari per comprendere la natura e le caratteristiche di urgenza delle richieste pervenute e instradarle affinché possano essere prese in carico coerentemente. ► Un **Digital Forensic Team**, composto da professionisti con competenze verticali ed esperienze specifiche in tutte le attività di Digital Forensic quali analisi dei log e degli eventi, malware forensic, network e system forensic, ecc., che coordina a sua volta ► una **Rete DFIR – Digital Forensic Incident Responder** capillare a livello nazionale, costituita dai *Forensic Experts* previsti dalla documentazione di gara che operano in qualità di professionisti qualificati e specializzati nell'acquisizione di evidenze digitali mediante strumenti e metodologie proprie dell'informatica forense. Tale rete è opportunamente dimensionata per poter rispondere tempestivamente anche in caso di incidenti sistemici che dovessero coinvolgere multiple Amministrazioni. ► Un **Incident Preparation Team**, composto da professionisti con esperienza pluriennale sul campo ed esperti di best practice, standard, metodologie e procedure di Security Incident Management, responsabile del supporto di carattere metodologico previsto nella fase di Incident Preparation e della quality assurance delle attività di Digital Forensics. L'Incident Preparation Team lavora inoltre a stretto contatto con l'**ONSP - Osservatorio normativo sulla security & privacy** (*cfr. § 3 Struttura Organizzativa*), al fine di intercettare e gestire eventuali evoluzioni normative che potrebbero avere impatti sulla gestione degli incidenti per le Amministrazioni, come ad esempio la pubblicazione di nuovi regolamenti / linee guida / modelli per la notifica degli stessi. ► Dei **centri di competenza**, organizzati secondo una struttura matriciale. Tale struttura prevede la collaborazione tra personale specializzato nelle infrastrutture tecnologiche IT e OT/IoT (*horizontal*) in termini, ad esempio, di sistemi operativi e applicazioni più comunemente attaccati, e di personale altamente qualificato in attività (*vertical*) di network forensics, system forensics e malware analysis Tale struttura a matrice consentirà al team operativo di poter combinare e usufruire in ogni momento delle conoscenze necessarie sia in termini di sistemi impattati, sia di strumenti e best practice per le attività di analisi.

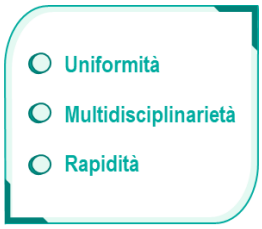


Il ***meccanismo di funzionamento*** del modello prevede che il Responsabile Tecnico (RT) agisca da interfaccia unica nei confronti del cliente, recependone le esigenze e indirizzandole verso i team operativi secondo i rispettivi ambiti di competenza e compatibilmente con il carattere di urgenza della richiesta. Il RT indirizza pertanto la richiesta verso l'*Incident Preparation Team* in caso di necessità di supporto metodologico e attiva il *Digital Forensic Team* in caso di attività di analisi post-mortem, avvalendosi eventualmente della *Rete DFIR* per l'acquisizione forense di dispositivi IT / OT / IoT localizzati sul territorio.

In relazione ai ***collegamenti con altre strutture*** il Responsabile Tecnico agisce da interfaccia nei confronti dei responsabili degli altri servizi previsti sia nel Lotto 1 sia nel Lotto 2. In particolare, il servizio di *Incident Management* è strettamente collegato al servizio di *Security Operation Center (SOC)* del Lotto 1 che gestisce operativamente gli incidenti di sicurezza a valle dei quali vengono effettuate le attività di analisi i cui risultati possono pertanto essere utilizzati sia come elemento di verifica indipendente circa l'efficace funzionamento del SOC, sia come "*lesson learned*" per promuovere il suo miglioramento continuo. Ulteriori elementi di collegamento con gli altri servizi possono essere identificati nell'ambito della compliance normativa, per quanto riguarda la gestione e notifica di *data breach* al Garante della Privacy, piuttosto che nell'ambito della Security Strategy, ove le "*lesson learned*" apprese possono essere utilizzate per indirizzare le scelte strategiche e i fabbisogni dell'organizzazione.

Efficacia e funzionalità del modello organizzativo adottato per le attività di analisi forense: Il modello organizzativo descritto ci consente di **indirizzare al meglio i fattori critici di successo** individuati dal RTI per il presente servizio, massimizzandone pertanto **l'efficacia**. ► *Multidisciplinarietà delle competenze a disposizione dell'analisi Forense*: la **presenza di team dedicati con competenze verticali**, che caratterizza il modello organizzativo illustrato, garantisce la copertura di tutte le competenze previste dal servizio in tutti i possibili contesti tecnologici che caratterizzano le diverse Amministrazioni. Ogni incidente rappresenta un *unicum* e può richiedere l'utilizzo di professionalità diverse, ad esempio in ambito

analisi dei log, analisi forense di malware, reti o sistemi, piuttosto che **acquisizione forense di una vasta gamma di dispositivi in ambito IT (Information Technology), OT (Operational Technology) o IoT (Internet of Things)**. L'accesso a **centri di competenza tematici** messi a disposizione dal RTI (*cfr. § 3 Struttura Organizzativa e § 14 Innovazione*) consente l'accesso a **professionalità diverse** da parte del RTI per affrontare problematiche complesse che necessitano analisi multidisciplinari eseguite da figure di competenza diversa. I nostri professionisti, infatti, possono vantare esperienza in tale settore a livello nazionale e internazionale, sia per l'**ambito Information Technology** (es. postazioni di lavoro, portatili, tablet, smartphone, server, NAS) con sistemi operativi Windows, macOS e Unix-like, sia per l'**ambito Operational Technology / IoT** (es. engineering workstation, field DB, SCADA, industrial PC) con sistemi operativi basati su Windows e Linux. Riteniamo tali competenze multidisciplinari fondamentali per Amministrazioni che, ad esempio, fanno largo uso di dispositivi IoT, come quelle che operano nel settore sanitario. Oltre a ciò, risulta fondamentale il **confronto con un network internazionale**, che fornirà ai professionisti impegnati sulle attività oggetto del contratto un canale privilegiato per fruire di informazioni sulle modalità di contrasto rispetto alle ultime minacce locali e internazionali, per analizzare minacce precedentemente sconosciute (es. malware reverse engineering, 0-day analysis, ecc.), nonché per confrontarsi su strumenti, tecnologie e best practice rispetto a casi d'uso. ► *Rapidità di esecuzione*: è elemento chiave per ► **acquisire il contenuto nelle memorie volatili** dei dispositivi impattati, fondamentale per la completezza dell'analisi forensica post-mortem ► **l'identificazione delle azioni di miglioramento utili a prevenire la reiterazione** dell'incidente o la sua diffusione a livello sistemico con impatto su altre PA ► **i processi di notifica previsti a livello normativo**, tra cui ad esempio ► **l'obbligo di notifica per i data breach** previsto dall'Art. 33 del GDPR entro le 72 ore dalla relativa scoperta, > l'obbligo di notifica "senza ingiustificato ritardo" previsto dalla Direttiva NIS per gli incidenti di sicurezza informatica, ► **i necessari processi di escalation verso le entità interne ed esterne** (inclusi CSIRT-Italia, organi di polizia giudiziaria, ecc.). **Il modello** da noi proposto **garantisce rapidità** di esecuzione sulla base di ① presenza della figura di Responsabile di Servizio **su base continuativa**, raggiungibile attraverso molteplici canali di comunicazione ② presenza di un **Digital Forensic Team dedicato**, che si avvale della presenza di una rete capillare sul territorio di DFIR, resa possibile dalla forte e ramificata presenza geografica del RTI sul territorio italiano; ③ predisposizione di **Go-Bag distribuite geograficamente sul territorio**, contenenti strumenti tecnologici essenziali per espletare le necessarie attività di acquisizione forense ad opera dei **DFIR** (es. write-blocker, chiavette USB *bootable* con sistemi operativi dedicati all'acquisizione forense, dischi con cifratura hardware su cui riversare i dati acquisiti, set di connettori/adattatori USB/SATA/ecc., set di cacciaviti, moduli di chain of custody prestampati, ecc.). Il modello garantisce inoltre la flessibilità organizzativa per gestire eventuali picchi di lavoro (*cfr. § 15 Flessibilità delle risorse*), e abilita la condivisione di conoscenze tra professionisti che supportano Amministrazioni diverse. ► *Uniformità dei processi di gestione degli incidenti di sicurezza tra PA*: in ambito sicurezza **è importante considerare le diverse PA come parte di un sistema integrato a livello Paese**, dialoganti tra loro attraverso una rete di CERT territoriali al fine di scambiarsi rapidamente informazioni e scongiurare incidenti a rilevanza sistemica, in coerenza con le linee guida AgID per lo sviluppo e la definizione del modello nazionale di riferimento. A tale scopo **il RTI persegue una diffusa uniformità di linguaggi, modelli e tassonomie** garantita tramite l'utilizzo di un modello organizzativo che **coniughi presenza locale con meccanismi di condivisione territoriale e coordinamento centrale**. L'utilizzo sistematico da parte del RTI **degli standard internazionali** in ambito Forense elencati in precedenza e di procedure rigorose e ispirate a queste best practice di settore, è elemento chiave per garantire sia l'uniformità dei processi tra PA sia la rigorosità del processo di indagine forense in se stesso. Il modello consente inoltre la gestione efficace dei **flussi di comunicazione interni e nei confronti dell'Amministrazione**, garantendo la presenza nel gruppo di lavoro di tutte le competenze necessarie per rispondere efficacemente a richieste specifiche e dialogare con tutte le parti coinvolte (vedi anche punto successivo)



7.2 Proposta di elaborazione di documento di "catena di custodia"

Per quanto riguarda la **catena di custodia**, abbiamo sviluppato un **modello realizzato ad hoc** ispirato alle best practice e affinato nel corso di centinaia di acquisizioni forensi effettuate sul campo. Riteniamo tale modello particolarmente efficace in quanto coniuga ► La **completezza di informazioni** necessaria a garantire la rigorosità del processo che recepisce, in particolare, i requisiti minimi in materia di Chain of Custody definiti all'interno dello standard ISO/IEC 27037:2012. ► La **facilità di utilizzo** che rappresenta un elemento fondamentale per non ingessare le attività di acquisizione forense svolte sul campo, spesso caratterizzate da tempistiche stringenti e condizioni logistiche precarie.

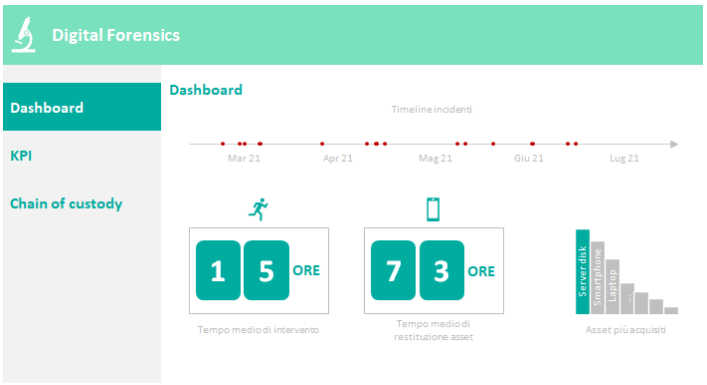
Rappresentazione delle informazioni qualitative e dimensionali oggetto di tracciamento. Il modello proposto di Catena di Custodia prevede **due sezioni**: ① una sezione di **Descrizione evidenze** dedicata all'inventariazione di tutti gli asset oggetto di acquisizione (es. dischi, smartphone, ecc.), attraverso l'assegnazione di un numero identificativo univoco (ID) e la raccolta di tutte le informazioni dimensionali e qualitative (es. modello, numero seriale, condizioni estetiche e funzionali, ecc.) necessarie a identificare in maniera puntuale ciascun asset e il suo stato al momento dell'acquisizione

Descrizione evidenze						
ID evidenza	**Quantità**	**Dimensioni**	**Descrizione (modello, # seriale, condizioni, danneggiamenti)**			
001	1	-	T480s	001	1	-

② una sezione **Catena di Custodia**, finalizzata a tracciare tutti i passaggi di consegna degli asset acquisiti attraverso l'annotazione del relativo ID, delle parti coinvolte (consegnatario e ricevente), delle motivazioni del passaggio di consegna e delle eventuali modifiche subite dall'asset nel periodo di custodia.

Catena di Custodia						
ID evidenza	**Data / ora**	**Consegnato da (firma e # documento di identità)**	**Preso in carico da (firma e # documento di identità)**	**Motivo del passaggio di custodia**	**Eventuali modifiche intercorse nel periodo**	**Note**
001	10/09/2021 ore 15:00	Mario Rossi	Giuseppe Verdi	Il passaggio di custodia è avvenuto in quanto …	Nessuna	-

Metteremo inoltre a disposizione delle Amministrazioni un applicativo web dedicato sul Portale della Fornitura per consentire un rapido accesso da parte delle PA aderenti. Sarà nostra premura caricare e mantenere aggiornati su tale applicativo tutti i documenti di Catena di Custodia, sia sotto forma di scansione, sia sotto forma di dati strutturati. In tale modo, **le Amministrazioni potranno in qualsiasi momento eseguire ricerche per conoscere lo stato di tutti e soli gli asset di cui sono proprietarie** che sono stati oggetto di acquisizione forense, nonché lo stato di completamento delle attività. Su una sezione dedicata del medesimo applicativo forniremo inoltre **statistiche, in forma aggregata e anonima, accessibili da tutte le amministrazioni**, che illustrano il tempo medio di intervento, il tempo medio di restituzione dell'asset, la quantità media di asset oggetto di acquisizione per indagine e le tipologie di asset maggiormente oggetto di acquisizione.

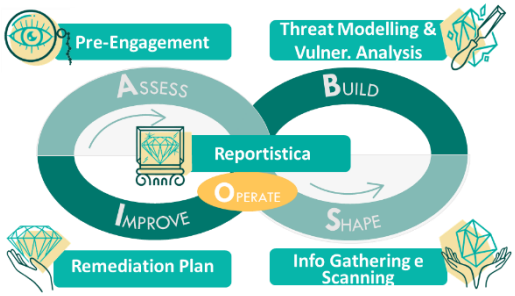


8 Proposta progettuale per il servizio "Penetration Testing"

"La sicurezza nell'Information Technology è come chiudere a chiave la casa o l'auto: non ferma i cattivi, ma li indirizza verso un obiettivo più facile" (Paul Herbka, Presidente dell'ISSA Advisory Board)

Obiettivi del servizio: obiettivo del servizio è fornire una soluzione in grado di garantire l'analisi e valutazione dei punti di vulnerabilità in termini di sicurezza rispetto ai sistemi IT dell'Amministrazione (Infrastrutture, Applicativi e IoT). In particolare, verranno condotti degli attacchi informatici simulati (preservando in ogni caso la disponibilità del servizio) al fine di evidenziare e classificare le diverse vulnerabilità. Il RTI nel corso degli anni grazie ad importati progetti di Information Security, in diversi settori di mercato, ha consolidato e maturato un approccio metodologico standard utile a presidiare: ► **gli ambiti infrastrutturali** (vulnerabilità interne/esterne al sistema, vulnerabilità delle reti wireless); ► **gli ambiti applicativi** (vulnerabilità delle applicazioni web e mobile, vulnerabilità delle API, phishing); ► **gli ambiti IoT** (vulnerabilità dell'infrastruttura di trasmissione e dei device connessi). Tale approccio è basato sulle *best practices* nazionali ed internazionali di settore come (a titolo esemplificativo e non esaustivo): **PTES** (Penetration Testing Execution Standard), **OWASP** (Open Source Web Application Security Project) e **OSSTMM** (Open Source Security Testing Methodology Manual), **MITRE ATT&CK** (Adversaries Tactics, Techniques and Common Knowledge), Unified Cyber Kill Chain, European Framework for Threat Intelligence-Based Ethical Red Teaming, G-7 Fundamental Elements of Threat-Led Penetration Testing e GFMA Framework for the Regulatory Use of penetration Testing and Red Teaming in the Finance Industry.

Metodologia: l'approccio metodologico IDEA, illustrato nel dettaglio nel paragrafo seguente, risulta caratterizzato, ove necessario, rispetto agli ambiti prima identificati (infrastrutturali, applicativi e IoT) e rispetto alle **cautele adottate nell'esecuzione dei penetration test** al fine di evitare il sovraccarico e/o l'indisponibilità dell'ambiente oggetto di valutazione e dei dati in coerenza con quanto previsto dalla normativa GDPR. Le evidenze raccolte saranno poi elaborate dagli specialisti messi a disposizione dal RTI all'Amministrazione all'interno di opportuni report (*cfr. § 8.2* Proposta di deliverable documentali con evidenza della rappresentazione delle informazioni qualitative e dimensionali oggetto di analisi).



Strumenti a supporto: gli strumenti messi a disposizione nell'**ambito infrastrutturale** sono nmap, Metasploit, netcat, wireshark, aircrack-ng, nell'**ambito applicativo** Burp Suite e Fortify e nell'**ambito IoT** Baudrate.py, Esptool, Flashrom, Minicom, Binwalk, Strings, IDAPro, Radare2, Qumu, Gatttool, hcitool, GNURadio e Killerbee.

8.1 Modalità di esecuzione del servizio: Penetration Testing e Cautele Adottate

Descriviamo nel dettaglio le modalità di esecuzione del servizio strutturate appositamente per *assicurarne concretezza ed efficacia*:

Assess **Assess cross-ambito**: in questa fase verrà svolta l'attività di **pre-engagement** necessaria alla definizione del **perimetro di scansione** in relazione all'oggetto di analisi.

Cross-ambito	Cautele adottate
Attività e Oggetti	**Metodi e Benefici**
Pre engagement sul perimetro di scansione: ambito di analisi, tempistiche, modalità di esecuzione dei test (white-box, grey-box o black-box), ambiente su cui svolgere le attività (produzione, UAT, integration, dev, ecc.) ed eventuali vincoli tecnici/operativi da considerare.	**Pen Ten Agreement – PTA** da concordare con i Key Stakeholders (es. CISO, Responsabile SOC, Responsabile NOC, ecc.): regole di ingaggio, aspetti operativi per lo svolgimento dell'attività, tempistiche, range temporali, perimetro tecnologico, ambienti target (sviluppo, pre-produzione ecc.) segmenti di rete da cui verranno effettuate le scansioni

Catena di erogazione end-to-end (es. Catena IoT: Device Connesso, Trasporto, APIs, Applicativo e Infrastruttura) incluse componenti applicative e infrastrutturali utili all'erogazione del servizio oggetto di valutazione.	e/o simulati gli attacchi a seconda modalità concordate (White/Grey Box Test). Il PTA ci consente di evitare disservizi dovuti a blocchi di segmenti di rete dovuti ad azioni di difesa dei firewall durante le attività di scansione, di concordare procedure di gestione di eventuali allarmi generati da sistemi SIEM, IDS o IPS e di attivare procedure automatiche/manuali causanti disservizi in risposta all'attacco simulato.

Shape specifica per ambito: in questa fase verrà svolta l'attività di **Info Gathering e Scanning** che ha l'obiettivo di raccogliere quante più informazioni possibili circa la *"superficie di attacco"* attraverso l'utilizzo di tecniche e strumenti tipici dell'ambito oggetto di analisi.

Ambito infrastrutturale	Cautele adottate
Attività e Oggetto	**Metodi e Benefici**
Approccio passivo tramite tecniche di OSINT e attivo tramite scansione di porte/servizi grazie all'utilizzo dei tool messi a disposizione del RTI (es. nmap, Metasploit, netcat, wireshark, aircrack-ng, ecc.). L'insieme delle informazioni raccolte, oltre a guidare le fasi successive della metodologia, permetterà tra le altre cose di individuare eventuali componenti non conformi alle policy aziendali (es. presenza servizi SMTP, NFS, FTP, SMB, ecc.).	Al fine di ridurre i possibili impatti derivanti dai Penetration Test le attività vengono concordare nel minimo dettaglio con i team di NOC e SOC e in ogni caso in fasce orario di scarso utilizzo/carico delle risorse. Le attività di scansione sono generalmente eseguite sugli ambienti di produzione, a meno di infrastrutture di tipo Virtuali e/o Software Defined per le quali si può operare su repliche fedeli dell'infrastruttura di esercizio.
Ambito Applicativo	**Cautele adottate**
Attività e Oggetto	**Metodi e Benefici**
Approccio passivo tramite l'integrazione e validazione delle informazioni esposte a livello applicativo da eventuali "registri" (es. SOA Registry, RESTful Service Registry, ecc.). **Approccio attivo** tramite la scansione di risorse esposte mediante tecniche di Crowling con l'utilizzo di strumenti specifici messi a disposizione dall'RTI (es. Burp Suite, Fortify, ecc.).	Attività condotte secondo quanto condiviso nel Pen Test Agreeement, garantendo il coordinamento delle attività tra NOC/SOC dell'Amministrazione (ove presenti) e il team di esperti messi a disposizione dal RTI. Qualora possibile tutte le attività vengono condotte su ambienti di collaudo/pre-produzione gestiti direttamente nell'ambito del SDLC e secondo i dettami del framework DevSecOps già presentato nell'ambito del servizio di Testing del Codice.
Ambito IoT	**Cautele adottate**
Attività e Oggetto	**Metodi e Benefici**
Approccio di **verifica dell'intera catena di erogazione del servizio** utilizzando le medesime tecniche già presentate per gli ambiti infrastrutturali e applicativi, valutando utleriori aspetti di Info Gathering e Scanning tipiche delle soluzioni protocollari di comunicazione adottate dai device connessi (es. Zigbee, zWave, 6LoWPAN, LPWAN, ecc.), attraverso l'adozione da parte del RTI di strumenti specifici (es. GNURadio). Vengono inoltre eseguite verifiche hardware del dispositivo come ad esempio: porte UART, tampering e JTAG Debbuing al fine di verificare eventuali superfici di attacco aggiuntive.	**Relativamente ai device connessi** è strettamente necessario valutare, grazie all'analisi della documentazione tecnica messa a disposizione dai vendor, i meccanismi di protezione automatica dei singoli dispositivi che se attivati potrebbero determinare il blocco del servizio. Inoltre, ove tecnicamente possibile, si effettuano delle scansioni passive sfruttando tecniche di analisi del traffico di tipo Port Mirroring e/o Tapping (replica fisica del dato) oltre che l'installazione e configurazione di device "gemelli" al fine di isolare quanto più possibile le attività di testing.

Build specifica per ambito: vengono svolte le attività di **Threat Modelling/Vulnerability Analysis al fine di identificare i differenti vettori di attacco e le superfici vulnerabili che verranno utilizzati per il PenTest, necessarie per condurre l'attività di Exploitation (e successivamente di Post-Exploitation) che sfrutta** tecniche e strumenti tipici dell'ambito oggetto di analisi indispensabili per confermare l'effettiva presenza di vulnerabilità oltre che il livello di criticità calcolata in base all'impatto che quest'ultime generano sul core-business dell'Amministrazione e su possibili dati di natura riservata

Ambito infrastrutturale	Cautele adottate
Attività e Oggetti	**Metodi e Benefici**

Utilizzo di exploit customizzati dai penetration tester di RTI anche attraverso l'utilizzo di strumenti a supporto quali: Metasploit, Exploit DB, ecc. Gli exploit customizzati sono stati sviluppati del team di penetration test di RTI che gode di un'esperienza pluriennale nel settore del penetration testing, e vengono utilizzati per attaccare anche i sistemi più aggiornati, bypassando i moderni meccanismi di protezione attivi e presenti sui sistemi quali Antivirus, EDR (Endpoint Detection and Response) ed EPP (Endpoint Protection Platform).	A seconda delle caratteristiche riconducibili agli ambienti infrastrutturali, le attività in questa fase verranno condotte adottando un approccio di tipo "Safe Check" (cfr. § 5), per cui per ogni vulnerabilità testata i relativi schemi di attacco non vengono effettivamente portati a termine salvo espresse indicazioni dell'Amministrazione. Nel caso vengano identificate vulnerabilità il cui sfruttamento porti all'indisponibilità dall'ambiente o dei dati, verrà verificata con l'Amministrazione la possibilità di condurre il test in un ambiente speculare. Nei penetration test di tipo black-box il comportamento in caso di potenziale sfruttamento di una vulnerabilità dovrà essere necessariamente condiviso a monte nel Pen test Agreement descritto sopra.
Ambito Applicativo	**Cautele adottate**
Attività e Oggetti	**Metodi e Benefici**
Attività condotta da un team di esperti messi a disposizione dell'Amministrazione che agiranno in relazione alle evidenze emerse in fase di shape e che, attraverso adozione di strumenti a supporto (Whireshark, Burp, ecc.) eseguiranno gli exploit applicativi. I test, eseguiti con il supporto dei centri di competenza del RTI, si baseranno su una base di conoscenza consolidata maturata tramite lo svolgimento di progettualità/attività di penetration test e agiranno sugli ambiti: Configuration e Deployment Management, Authentication, Authorization, Identity Management, Session Handling, Service Exposure, Input Validation, Error/Exception Handling, Weak Cryptography, Business Logic	Sfruttando la catena e gli strumenti di CI/CD, ed in linea con il processo di SDLC descritto nell'ambito del servizio di Testing del Codice, le attività di penetration test verranno svolte su aree dedicate. Tali ambienti saranno gestiti, ove possibile, virtualmente attraverso l'adozione di strumenti "infrastructure-as-a-code" (es. open-stack) e con l'utilizzo del Continuous Integration Server Jenkins *(cfr. § 6Proposta progettuale per il servizio "Testing Del Codice")* per la parte di deploy automation al fine di garantire il completo isolamento con gli ambienti di esercizio e evitare eventi di Data Corruption.
Ambito IoT	**Cautele adottate**
Attività e Oggetti	**Metodi e Benefici**
Data la peculiarità d'ambito, l'attività viene condotta a livello hardware (agendo fisicamente su eventuali porte UART aperte JTAG exploitation e Dumping Flash Memory), a livello firmware (agendo attraverso tecniche di reverse engineering, forced upgrade, Binary Analysis) e a livello radio (agendo a livello protocollare attraverso tecniche di sniffing-modifying-replaying di pacchetti o tecniche di jamming) attraverso l'utilizzo di alcuni strumenti specifici (livello hardware: Baudrate.py, Esptool, Flashrom, Minicom e Screen; livello firmware: Binwalk, Strings, IDAPro, Radare2 e Qumu; livello radio: Gatttool, hcitool, GNURadio e Killerbee).	Analogamente a quanto già descritto nell'ambito delle attività della fase di Shape, al fine di ridurre al minimo gli impatti sull'infrastruttura di esercizio (intera catena), il RTI metterà a disposizione i propri centri di competenza e laboratori di testing per simulare in ambiente controllato le condizioni di esercizio del singolo servizio utilizzando device IoT di test.

Improve & Operate cross-ambito: in questa fase verranno raccordate tutte le informazioni raccolte nelle precedenti fasi e generati dei **deliverables inerenti alle attività svolte con informazioni qualitative e dimensionali fruibili sia da personale tecnico sia non tecnico**. In questa fase verrà inoltre redatto un **Remediation plan** che permetterà all'Amministrazione di risolvere le falle di sicurezza riscontrate e fornirà delle raccomandazioni di sicurezza per ottenere un improvement della security posture dell'intera organizzazione. In particolare, **l'attività di Reportistica sarà finalizzata alla raccolta delle evidenze relative alle vulnerabilità confermat**e. Queste verranno riportate step-by-step in maniera da poter essere riprodotte e verificabili in caso di eventuali audit. La classificazione delle vulnerabilità prenderà in considerazione almeno le seguenti dimensioni: Impegno richiesto ad un attaccante per sfruttare con successo la vulnerabilità, impatto che si avrebbe sul business aziendale qualora la vulnerabilità venisse effettivamente confermata (rischio legale, di business, di immagine, di compliance, operativo) e Impatto in termini di Riservatezza, Integrità e Disponibilità del dato (coerentemente anche a quanto previsto dalla normativa GDPR). Le evidenze raccolte lungo lo svolgimento dell'iter metodologico saranno poi elaborate dagli specialisti messi a disposizione dal RTI all'Amministrazione all'interno di opportuni report illustrati di seguito.

8.2 Proposta di deliverable documentali con evidenza della rappresentazione delle informazioni qualitative e dimensionali oggetto di analisi

L'obiettivo della seguente proposta legata alla fase di Reporting è quello di **fornire una visione dettagliata ed esaustiva dei contenuti che verranno forniti all'interno dei deliverable documentali (o reportistica)**. Tali deliverable conterranno le evidenze delle azioni intraprese all'interno delle fasi operative precedenti, l'effetto di tali azioni ed i relativi risultati. Verranno inoltre specificati i singoli passi necessari intrapresi per sfruttare le vulnerabilità rilevate. La classificazione e la presentazione delle singole vulnerabilità identificate seguiranno le seguenti classificazioni di Severity Levels, in accordo ai framework internazionale adottati e citati in precedenza.

Severity score	Description
Critical (9.0 – 10.0)	Vulnerabilità che permette ad un attaccante di ottenere il controllo completo di una risorsa informatica (es. un server web) o permette di ottenere dati business-critical o legalmente rilevanti (es. dati protetti da leggi sulla privacy).
High (7.0 – 8.9)	Vulnerabilità che permette ad un attaccante di compromettere la riservatezza/integrità/disponibilità dei dati dell'utente o delle risorse.
Medium (4.0 – 6.9)	Vulnerabilità o esposizione di dati che non portano ad compromissione diretta dall'applicazione, ma possono essere utili all'attaccante per compromettere il target.
Low (0.1 – 3.9)	Vulnerabilità o esposizione di dati non rilevanti, ma che rappresentano una non conformità delle best practice di sicurezza seppur non introducono un rischio rilevante immediato.

I seguenti deliverable documentali descriveranno in modo efficace il dettaglio delle attività di Penetration Test eseguite sui target oggetto di analisi: ►**Executive Report: overview ad alto livello delle vulnerabilità riscontrate**, con informazioni dimensionali quali il numero totale delle vulnerabilità riscontrate e la percentuale delle vulnerabilità trovate suddivisa per severity critica, alta, media e bassa. Sarà inoltre presente un codice che permetterà di identificare univocamente ognuna delle diverse vulnerabilità nel caso di necessità da parte dell'Amministrazione. Il documento sarà fruibile anche da personale non tecnico. ►**Technical Report: dettagli tecnici dell'attività di PT svolta.** Per ognuna delle vulnerabilità riscontrate durante l'attività, si forniscono contenuti dimensionali relativi al **numero di risorse impattate da ogni vulnerabilità, numero di parametri vulnerabili, numero di servizi esposti vulnerabili e numero di componenti affette da vulnerabilità**. Viene mostrato il dettaglio sulla vulnerabilità rilevata e i contenuti qualitativi come immagini di tool e opportuna configurazione per sfruttare una vulnerabilità, porzioni di codice utilizzate per attaccare i sistemi, tecniche utilizzate per bypassare AV, EDR o EPP, azioni e comandi eseguiti sui sistemi oggetto di analisi. Il report consente la comprensione di ogni step dell'attacco eseguito in maniera puntuale e precisa, rendendo il processo chiaro ed eventualmente ripetibile. ►**Remediation Plan: misure da mettere in atto** per ogni vulnerabilità individuata, customizzate per lo specifico target oggetto di analisi e necessarie per sanare il problema di sicurezza rilevato e renderlo non più sfruttabile. Arricchito da una tabella riassuntiva che contiene l'elenco delle vulnerabilità ordinate secondo la gravità in modo da consentire la prioritizzazione delle bonifiche da applicare.

Inoltre, all'interno di ognuno dei deliverable saranno presenti sezioni con informazioni necessarie per contestualizzare quanto svolto: ►**Scope**: informazioni dimensionali relative al numero di target oggetto di analisi, finestre temporali concordate per lo svolgimento dei test, numero di utenze fornite, indirizzi sorgente e destinazione specifici dell'attività. Permette di consultare le informazioni relative a quanto concordato in fase di **Assess** in maniera concisa, efficace e schematica, permettendo ad eventuali auditor esterni di verificare in maniera semplice e concreta quanto svolto durante le attività di Penetration test. ►**Tools**: informazioni qualitative su tools e tecniche utilizzate durante le attività di Penetration Test, che consentono l'installazione e la configurazione dei tool necessari per replicare gli esatti step che hanno portato allo sfruttamento delle vulnerabilità identificate, rendendo il processo completamente trasparente e riproducibile sia per necessità in fase di audit sia per necessità durante la fase di applicazione delle bonifiche suggerite dal team RTI.

9 Proposta progettuale per il servizio "Compliance Normativa"

"Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino della nostra società"
(S. Rodotà)

Il contesto straordinario in cui opera l'intero sistema Paese e, di riflesso, la Pubblica Amministrazione, richiede rapidità ed efficacia senza precedenti nell'erogazione di servizi alla cittadinanza, anche alla luce degli importanti pacchetti di misure stanziate a livello comunitario per fronteggiare l'emergenza sanitaria e socioeconomica. In tale scenario, il servizio di **"Compliance Normativa"** supportato dal Centro di competenza Risk & Compliance consente alle Amministrazioni di sopperire alle criticità e ai limiti che quotidianamente si trovano a fronteggiare con riferimento alla protezione dei dati personali. Sulla base della nostra esperienza, infatti: ► la privacy è concepita spesso come un **mero adempimento normativo**, e non ne sono valorizzati **gli aspetti etici e tecnologici** che consentirebbero all'Amministrazione di perseguire in maniera strutturata il percorso verso la trasformazione e innovazione digitale; ► **è spesso carente l'approccio "federativo"** nella gestione di servizi e banche dati pubbliche, ovvero le Amministrazioni che erogano servizi affini o che interrogano vicendevolmente le proprie banche dati, dovrebbero cooperare per indirizzare fin dal principio i requisiti di privacy; ► **non sempre è prevista l'adeguata interoperabilità** e messa a fattor comune delle banche dati pubbliche; tali elementi consentirebbero di ottenere risultati significativi in termini di fiducia, efficacia e trasparenza che la cittadinanza richiede al Sistema Paese.

Obiettivi del servizio: la nostra **profonda conoscenza dei processi in ambito privacy**, declinati in funzione delle specificità dei singoli Comparti della PA, ci consente di offrire un servizio finalizzato non solo a garantire il raggiungimento della piena "compliance normativa" ma, in aggiunta, **l'adozione efficace di prassi e strumenti di governo e gestione dei trattamenti dei dati personali**, con un approccio scalabile in funzione degli scenari di rischio applicabili alle finalità di trattamento.

Metodologia: con riferimento all'approccio metodologico, riteniamo fondamentale **distinguere**, nella complice normativa, **tra attività puntuali (o se necessario ricorsive) e continuative**. L'approccio puntuale (di cui alle prime 4 fasi di seguito declinate) consente un **supporto end-to-end all'Amministrazione**, a partire dall'analisi del contesto fino ad arrivare al supporto nell'implementazione delle azioni correttive. L'approccio continuativo (di cui alla fase Operate sotto declinata), invece, **garantisce la sistematicità delle attività day-by-day, in linea con quanto prescritto** dalla normativa

privacy in relazione al continuo miglioramento dei presidi di sicurezza. Le attività seguono il framework Idea consolidato già in numerose esperienze presso primarie Amministrazioni Pubbliche:

Assess **Comprensione contesto:** la fase di Assess è finalizzata alla comprensione del contesto, in relazione ai processi di trattamento dei dati personali con un focus sul perimetro IT, nonché alla valutazione del livello di maturità attuale dell'Amministrazione in ambito privacy;

Shape **Gap Analysis:** la fase di Shape è finalizzata alla definizione e stima in termini di criticità degli scostamenti (Gap Analysis) tra il livello di maturità attuale e il livello di maturità atteso dell'Amministrazione, dove quest'ultimo rappresenta il livello di maturità che si intende raggiungere, in relazione ai requisiti per i quali non è stata raggiunta la piena conformità, nonché degli obiettivi strategici da perseguire;

Build **Piano di interventi:** la fase di Build consente di identificare le azioni di intervento, formalizzate all'interno di un apposito Piano di Interventi oggetto di continuo monitoraggio e miglioramento, da implementare per perseguire il livello di maturità atteso;

Improve **Azioni correttive:** la fase di Improve è finalizzata al supporto nell'implementazione delle azioni correttive incluse nel Piano di Intervento;

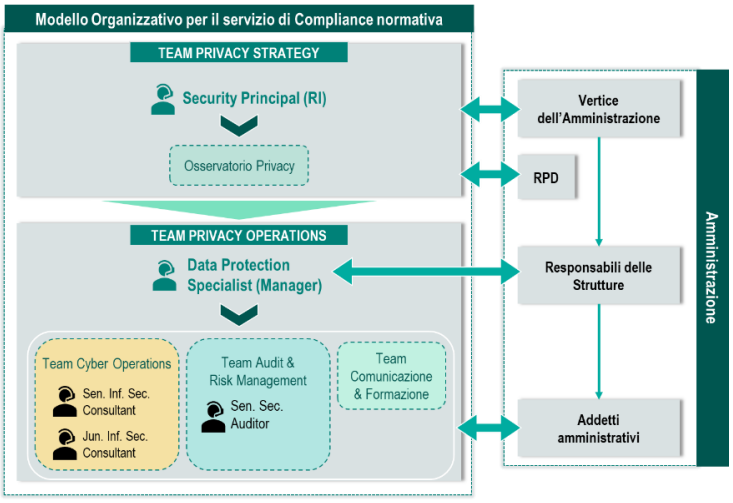
Operate **Supporto e gestione:** la fase di Operate è finalizzata a garantire un supporto specialistico nella gestione day-by-day non solo degli adempimenti privacy, ma anche nel perseguimento degli obiettivi e indirizzi strategici dell'Amministrazione.

Strumenti di automazione e governo: al fine di garantire il governo dei processi di trattamento dei dati personali, nonché assicurare il rispetto degli adempimenti normativi, mettiamo a disposizione una **suite di strumenti di Privacy Management** che integra soluzioni custom per la singola Amministrazione con strumenti di Office Automation; si tratta di un insieme di moduli per l'automazione, governo e monitoraggio di tutti gli adempimenti privacy, quali: **gestione del Registro delle attività di trattamento; gestione dei data breach, integrazione dei principi di Privacy by Design & by Default, esecuzione della Data Protection Impact Assessment.**

Standard adottati: per l'esecuzione delle attività, ricorriamo a metodologie e strumenti definiti in linea con best practice e standard internazionali. Nello specifico, il nostro approccio risulta essere basato sull'analisi del rischio, ovvero, le misure di sicurezza sono commisurate ai rischi per i diritti e le libertà degli interessati. A tale scopo, **mutuiamo nei nostri strumenti i principi degli standard più recenti e all'avanguardia in ambito privacy e cybersecurity, quali, a titolo esemplificativo, ISO/IEC 27701:2019, ISO/IEC 29134:2017, ISO/IEC 31000:2018, Enisa Threat Landscape Report, ecc.**

9.1 Modello organizzativo, elementi di efficacia e funzionalità

Intendiamo adottare il seguente modello organizzativo:



Team Privacy Strategy (Service Unit): il Team di Privacy Strategy fornisce supporto nel definire, indirizzare e migliorare la strategia dell'Amministrazione con riferimento a obiettivi e linee di indirizzo da perseguire in ambito privacy. Esso è costituito da: ► **Security Principal**: esso costituisce il punto di contatto unico con il vertice Amministrativo e con il Responsabile Protezione Dati ("RPD" o "DPO") dell'Amministrazione. Supporta l'Amministrazione in occasione di tavoli tecnici e/o incontri istituzionali con l'Autorità di Controllo e con i RPD di altre Amministrazioni. Garantisce il rispetto, in ciascuna attività del Servizio eseguita dal Team Privacy Operations, degli indirizzi strategici che l'Amministrazione persegue in ambito privacy; ► **Osservatorio Privacy**: esegue continua sorveglianza normativa, analisi e adozione delle nuove prassi e strumenti in ambito privacy in linea con nuovi standard e framework internazionali. La tempestiva rilevazione di trend ed elementi innovativi nelle prassi internazionali è funzionale alla definizione di indirizzi strategici all'avanguardia. In caso di evoluzioni normative, le comunica al Team Privacy Operations cui fornisce supporto nella valutazione degli impatti per l'Amministrazione in termini di adempimenti privacy. **Team Privacy Operations (Service Unit)** verifica periodicamente il livello di maturità attuale dell'Amministrazione, anche alla luce delle evoluzioni normative comunicate dall'Osservatorio Privacy e supporta l'implementazione delle azioni correttive. Esso è composto da:

DATA PROTECTION SPECIALIST

Manager responsabile del coordinamento del **Team Privacy Operations**; si interfaccia quotidianamente con la struttura del Titolare per il tramite dei Responsabili delle Funzioni/Direzioni dell'Amministrazione e attiva prontamente i sotto-team Cyber, Audit & Risk Management e Comunicazione & Formazione in relazione alle attività di privacy by design, DPIA, Privacy Culture e aggiornamento del registro dei trattamenti, laddove necessario

TEAM CYBER OPERATIONS

Costituito da **Senior Information Security Consultant** e **Junior Information Security Consultant**, mette a disposizione competenze specialistiche in ambito Cyber security sia dal punto di vista della security governance, sia di conoscenza di prassi e soluzioni tecnologiche per la tutela dei dati (e.g. cifratura, data retention, strong authentication, Identity and Access Management). Gli scostamenti rilevati in termini di misure di sicurezza ICT sono prontamente comunicati al Team Privacy Strategy che li declina in nuovi indirizzi strategici per l'innalzamento del livello di maturità dell'Amministrazione dal punto di vista tecnologico

TEAM AUDIT & RISK MANAGEMENT

Costituito dal **Senior Security Auditor**, mette a disposizione dell'Amministrazione comprovata esperienza nell'applicazione delle metodologie di audit e privacy risk management, che consentono di verificare periodicamente l'osservanza della normativa da parte dell'Amministrazione e contribuire alla definizione di azioni correttive secondo un approccio risk-based. Gli scostamenti rilevati in termini di mitigazione dei rischi sono prontamente comunicati al Team Privacy Strategy che li declina in nuovi indirizzi strategici per l'innalzamento del livello di maturità con riferimento alle metodologie di audit

TEAM COMUNICAZIONE E FORMAZIONE

Composto da **professionisti con comprovata esperienza nei rapporti istituzionali tra differenti PA**, mediante la partecipazione a tavoli tecnici, comitati, etc. Inoltre, i nostri professionisti applicano metodologie di **culture & awareness** avanzate per aumentare la sensibilità privacy dei funzionari amministrativi. Il dialogo costante tra Team Comunicazione & Formazione e Team Privacy Strategy consente di integrare la "privacy culture" negli indirizzi strategici dell'Amministrazione.

Efficacia e funzionalità del modello organizzativo: alla luce del disposto normativo privacy nazionale e comunitario, delle prassi più evolute sul panorama internazionale e, da ultimo, delle difficoltà che le Amministrazioni si trovano a fronteggiare nell'operatività quotidiana –in precedenza rilevate – riteniamo che i **fattori critici di successo** per l'adozione di un modello di gestione della privacy maturo siano: ▶ *adottare modalità e canali di comunicazione efficace e tempestiva* tra il Titolare (i.e. l'Amministrazione) e il RPD al fine di innescare prontamente gli adempimenti privacy; ▶ *concepire procedure e misure per la protezione dei dati* non solo come mezzo per il raggiungimento della compliance normativa e, conseguentemente, per evitare le sanzioni, ma come strumento atto a perseguire gli indirizzi strategici che l'Amministrazione si è posta in termini di digitalizzazione e innovazione; ▶ *essere in grado di rilevare tempestivamente evoluzioni normative*, valutarne applicabilità e impatti sui processi dell'Amministrazione; ▶ disporre di un *centro di controllo che indirizzi gli aspetti privacy* in maniera complessiva; ▶ integrare nei processi dell'Amministrazione la *"cultura del dato" a tutti i livelli e ambiti di intervento*. In tale contesto, il **modello organizzativo** da noi proposto si rileva particolarmente **efficace e funzionale** nell'indirizzare e abilitare i sopramenzionati fattori critici di successo:

Comunicazione efficace

Prevediamo risorse e team dedicati: il Data Protection Specialist e, nella sua interezza, il Competence Center Risk & Compliance supporta day-by-day nelle operatività quotidiana le singole Direzioni/Funzioni che costituiscono la struttura del Titolare; in tal modo, siamo in grado di rilevare near real-time variazioni ai processi esistenti o la definizione di nuovi servizi/processi di trattamento che richiedono l'avvio di attività di privacy by design & by default e di valutazione dei rischi ex artt. 25, 32 e 35 del GDPR. Non appena rilevata un'esigenza in tal senso, avviene la comunicazione verso il Team Privacy Strategy, che coopera a stretto contatto con il RPD al fine di attivare i relativi adempimenti *privacy*

Visione evoluta delle procedure e misure di privacy

Il modello organizzativo dimostra **efficacia e flessibilità**, garantite dalla presenza del Team di Privacy Strategy, in grado di tenere in considerazione non solo i requisiti normativi, ma anche gli **obiettivi** che si intende perseguire nel breve, medio e lungo termine, tra cui: ① **semplificazione dei processi di raccolta di dati personali** (es. laddove opportuno, incrementare il ricorso all'autodichiarazione e rafforzare i controlli ex post circa la veridicità delle informazioni dei cittadini); ② **potenziamento dell'interoperabilità tecnica** tra banche dati pubbliche; ③ **efficienza nelle procedure di aggiornamento ed esattezza** dei dati personali al fine di ridurre i rischi legati a erroneo rigetto di domande/istanze; ④ **principi di Privacy by Design & by Default** su perimetro IT; integrazione nei processi aziendali della "cultura del dato" di cui al successivo punto ⑤, ovvero del rispetto della riservatezza dei dati personali al fine di mitigarne i rischi per gli interessati

Capacità di rilevare e valutare gli impatti delle evoluzioni normative

Il nostro modello si rivela particolarmente **efficace in quanto prevede l'Osservatorio Privacy**, che valuta applicabilità e impatti per ciascuna evoluzione normativa e/o nuovo standard, emettendo un bollettino verso tutti i soggetti interni e attivando il Competence Center Risk & Compliance per il raggiungimento della compliance

Centro di controllo degli aspetti di privacy

Riteniamo doveroso convergere significativamente sull'interoperabilità tecnica dei sistemi/banche dati di diverse Amministrazioni; a tal fine, supportiamo l'Amministrazione nel costituire un centro di controllo con tavoli tecnici con altre PA al fine di stabilire protocolli di comunicazione e scambio di dati in conformità a: ① **Provvedimento del Garante per la Protezione dei Dati personali** del 2 luglio 2015 – Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche; ② **Linea di indirizzo sull'interoperabilità tecnica delle Pubbliche Amministrazioni di AgID**; ③ **Codice dell'Amministrazione digitale** di cui al Decreto Legislativo 7 marzo 2005, n. 82. L'esperienza di applicazione dei principi inclusi nei suddetti riferimenti normativi ci consente di supportare l'Amministrazione nell'identificazione di adeguate soluzioni in termini di **architetture API** (Application programming interface), **servizi REST** (Representational State Transfer), **accessi selettivi ai dati** e, in generale, misure di sicurezza tecniche (backup, cifratura, log management, network security, ecc.)

Cultura del dato

Il nostro modello organizzativo prevede un t**eam dedicato di Comunicazione & Formazione**, che eroga un servizio di **Privacy Culture & Awareness** che include l'erogazione di sessioni formative rivolte a tutti i livelli del personale amministrativo con un approccio di experiential learning cycle, ovvero mediante lo strumento del workshop in cui i referenti simulano l'applicazione delle procedure privacy interne (es. privacy by design e DPIA) a casi d'uso attinenti alla tipologia di Comparto della PA

9.2 Rapporto di compliance

Nel corso dell'erogazione del Servizio, predisponiamo e aggiorniamo sistematicamente il Rapporto di Compliance, da intendersi non come un semplice documento, ma come un **tool che fornisce una vista real-time dello stato di maturità dell'Amministrazione in ambito privacy e dello stato di avanzamento delle azioni correttive.** Al fine di garantire immediatezza ed efficacia in termini di fruibilità e accessibilità**, il Rapporto di Compliance costituisce una sezione del Portale della Fornitura**, che consente **il download in formati open delle singole sezioni sottostanti**. A ciascuna funzionalità del tool corrisponde un'area all'interno del Portale, quali, ad esempio: ► **criteri di verifica** laddove è possibile visionare la metodologia adottata per la selezione dei trattamenti da sottoporre ad Assessment, quali, ad esempio, criticità dei dati trattati (es. categorie particolari ex art. 9 GDPR) e di interessati coinvolti (es. soggetti vulnerabili o minori) o delle modalità di trattamento (es. trattamento su larga scala, correlazione di banche dati oltre le aspettative degli interessati, ecc.); inoltre, sono previsti collegamenti via web link al corpo normativo applicabile, quali il Regolamento UE 2016/679, la normativa nazionale in materia di privacy (es. D.lgs. 196 del 2003 e ss.mm.ii, Provvedimenti del Garante per la Protezione dei Dati Personali) e agli standard internazionali di riferimento (es., ISO/IEC 27017:2019, ISO/IEC 27001:2013, ISO/IEC 27701:2019). Il tool mette a disposizione funzionalità di "filtraggio" che consentono di personalizzare la ricerca in funzione degli ambiti di interesse, ovvero standard e fonti normative; ► **risultanze delle attività** che illustra gli esiti delle attività di valutazione della maturità e della fase di Shape. Sono resi disponibili i documenti ed evidenze raccolte e analizzate in fase di Assess, nonché prodotte schede di dettaglio per ciascun gap rilevato. Il tool consente di eseguire attività di benchmarking rispetto ad altre PA (naturalmente in forma anonima) per verificare il posizionamento dell'Amministrazione rispetto al panorama pubblico italiano nella sua interezza e/o a singoli Comparti; inoltre, è possibile testare il livello di maturità rispetto a una singola fonte normativa e generare report personalizzati in termini di arco temporale preso in considerazione, ambiti di controllo di interesse e per singoli processi/sistemi dell'Amministrazione; ► **conclusioni delle attività di verifica**: consente la navigazione del Piano di interventi definiti per perseguire il livello di maturità atteso. Sono messe a disposizione funzionalità che consentono di monitorare lo stato di effettiva implementazione delle azioni, nonché eseguire il download di report executive summary o di dettaglio per attività di relazione periodica del RPD e di altri referenti amministrativi interessati verso il vertice amministrativo o materiale di supporto in caso di visita ispettiva da parte dell'Autorità di Controllo. Da ultimo, il tool consente di generare analisi storiche circa l'evoluzione nel tempo del livello di maturità privacy dell'Amministrazione fornendo highlight sulle principali variazioni in termini di processi, procedure, prassi e soluzioni tecniche adottate per sanare i gap identificati in passato.

10 Portale della Fornitura

"L'utilizzo di canali di comunicazione rapidi e diretti fra amministrazioni e fornitori, o fra questi e gli organismi di coordinamento e controllo, rappresenta un fattore determinante per garantire il rispetto dei principi di economicità, efficacia ed efficienza dell'azione amministrativa."
(Corollario del buon andamento dell'azione amministrativa (Legge 241/1990, art. 97 della Costituzione Italiana)

Il **Portale della fornitura (PDF)** che il RTI propone è stato concepito per diventare a tutti gli effetti il "luogo di incontro" di tutti gli attori coinvolti a diverso titolo nella fornitura. È stato progettato in ottica **multicanale** (siti, portali, blog, social network, mobile, ecc.), raggiungibile tramite Internet, per consentire alle singole Amministrazioni ed agli Organismi di coordinamento e controllo di attivare e governare agevolmente i servizi e di **promuovere la condivisione** e l'esperienza maturata nelle singole iniziative. Strutturato sulla base delle aree previste da Capitolato, il Portale è stato arricchito di numerosi elementi migliorativi, grazie ad una **progettazione user centered** basata sui principi di facilità di utilizzo e rilevanza rispetto alle esigenze dell'utente. I principali obiettivi del PDF sono: ► **Informare e coinvolgere le Amministrazioni**, perché aderiscano all'Accordo Quadro; ► **migliorare il processo di interazione e collaborazione tra gli stakeholder** per la condivisione di documenti e contenuti; ► indirizzare un **confronto su esperienze e iniziative di interesse comune** per favorire il riuso delle soluzioni; ► gestire l'intero **ciclo di vita degli affidamenti** e controllare e monitorare la **conduzione**

dei contratti esecutivi; ► **garantire la condivisione della documentazione** e la messa a disposizione di cruscotti grafici riassuntivi in merito all'andamento di tutti i Contratti Esecutivi; ► consentire a Consip ed AgID di svolgere le proprie **funzioni di monitoraggio** sulla qualità dei servizi erogati in AQ. Il Portale sarà implementato con certificato per la navigazione esclusiva in HTTPS e configurato con certificati non self-signed; sarà cura del RTI assicurare i servizi di gestione dei contenuti, delle utenze, la messa a disposizione del manuale d'uso e il servizio di assistenza all'utente.

10.1 Soluzioni tecnologiche e funzionalità del Portale della fornitura e strumenti di analisi dei dati e reporting

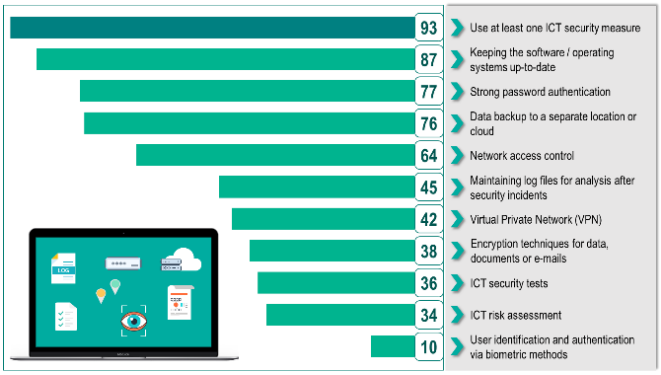
Il RTI vuole offrire attraverso il PDF un vero e proprio **kit di strumenti, funzionalità e soluzioni tecnologiche a supporto delle diverse Amministrazioni**, di Consip, degli Organismi di Coordinamento e Controllo e più in generale di tutti gli stakeholder interessati. Di seguito un quadro sinottico per ogni area del portale in cui sono rappresentati gli strumenti, le funzionalità a disposizione e le soluzioni tecnologiche adottate.

Area	Funzionalità	Strumenti	Soluzione tecnologica
Comunicazione Area ad accesso pubblico del portale per informazione e promozione dei servizi sull'AQ e sui progetti in esecuzione	Funzionalità di ricerca tra gli obiettivi dell'Accordo Quadro Funzionalità di ricerca e consultazione di Faq Funzionalità di ricerca e consultazione di best practice, linee guida, contenuti normativi, news e aggiornamenti in ambito cyber security Funzionalità di ricerca e consultazione di best practice, linee guida, contenuti normativi, news e aggiornamenti in ambito cyber security Funzionalità di ricerca e consultazione Library di case studies in termini di evoluzione delle minacce "cyber" e dei relativi impatti, sia dal punto di vista quantitativo che da quello qualitativo	Knowledge Base	WordPress
	Funzionalità di ricerca e consultazione di dati di libero accesso attraverso cruscotti	Analytics Dashboard e Reporting	KNOWAGE, OpenDataSoft, wpDataTables
	Funzionalità di supporto utente attraverso Chatbot Funzionalità di gestione delle anagrafiche Funzionalità di gestione delle richieste di supporto degli utenti	Customer Relationship Management	odoo
Informativa Area ad accesso pubblico del portale per supportare le PA nel processo di adesione all'accordo. Contiene inoltre un'area privata per la profilazione delle Amministrazioni che hanno aderito all'accordo	Funzionalità di registrazione Funzionalità di configurazione profilo Funzionalità di ricerca e fruizione di contenuti informativi	Self Assessment	Alfresco, WordPress, Formidable Forms, OpenAM
	Funzionalità "wizard" che semplificano le procedure di adesione ai servizi guidando l'utente nella compilazione del Piano dei Fabbisogni attraverso l'utilizzo di modulistica	Editor modulistica, wizard	<form.io>
	Funzionalità di consultazione e profilazione per le amministrazioni che hanno aderito ai servizi Funzionalità di consultazione dei servizi consigliati segmentati sulla base delle caratteristiche del self-assessment	Profilazione PA	Alfresco, OpenAM
Osservatorio Area che consente alle Amministrazioni, ad AgID ed a Consip di svolgere le funzioni di monitoraggio della qualità	Funzionalità di analisi e monitoraggio con un cono di visibilità specifico su singoli Piani dei Fabbisogni, sull'andamento dei loro indicatori di performance e percentuale di aderenza degli interventi al Piano Triennale per l'Informatica della PA, aggiornato al triennio 2020-2022 Funzionalità di alert e strumenti di segnalazione nel caso di mancato rispetto degli SLA Funzionalità di conversazione diretta con la PA interessata e con il Fornitore al fine di chiarire il rilievo effettivo e qualitativo	Analytics Dashboard e Reporting	OpenDataSoft, wpDataTables, KNOWAGE

Project Management Area ad accesso riservato e profilato per le singole Amministrazioni tramite la quale è possibile disporre degli strumenti di attivazione, pianificazione e gestione delle singole iniziative progettuali	Funzionalità di pianificazione e monitoraggio delle attività amministrative, gestionali e operativo delle proprie iniziative Funzioni di governo e monitoraggio di tutti gli adempimenti privacy	Planner utente	Upstream
	Funzionalità di classificazione, gestione e l'archiviazione di tutti i documenti prodotti nell'ambito dello specifico progetto e nei singoli contratti esecutivi	Document management	Upstream
	Funzionalità di gestione delle singole iniziative progettuali attraverso l'elaborazione di cruscotti di avanzamento per ciascuna iniziativa progettuale	Project management	Upstream
Collaborazione e monitoraggio Area che contiene gli strumenti di promozione, collaborazione e condivisione tra le PA e gli strumenti di monitoraggio e governo della fornitura	Funzionalità di social blogging; Funzionalità di forum di discussione; Funzionalità di chat; Funzionalità di mailing list; Funzionalità di talk & training; Funzionalità di wiki	Collaboration	Open2.0
	Funzionalità di analisi e monitoraggio di dati qualitativi e quantitativi (es. controlli ABSC "Agid Basic Security Control" sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dei servizi di gara	Analytics Dashboard e Reporting	OpenDataSoft; wpDataTables; KNOWAGE
	Funzionalità di predisposizione, compilazione e analisi di survey di customer satisfaction Funzionalità di reporting su soddisfazione utente; Funzionalità di analisi della soddisfazione utente rilevata	Analytics Dashboard e Reporting	SurveyMonkey

Il Portale si configura come strumento di contatto e di lavoro in grado di assicurare il costante monitoraggio e la valutazione dell'andamento delle attività; ogni informazione gestita nell'ambito dei servizi sarà quindi classificata, organizzata, storicizzata e resa accessibile.

Il RTI dispone di un'ampia gamma di soluzioni tecnologiche per facilitare la raccolta, la strutturazione, la visualizzazione e la condivisione delle informazioni rilevanti; si propone l'utilizzo di strumenti **di analisi dati e reporting leader di mercato**: ► **OpenDataSoft® e Knowage®**: strumenti innovativi per la gestione e l'analisi di Basi Dati (anche di grandi dimensioni), attraverso l'utilizzo di workflow ripetibili; tipicamente sono utilizzati per aspetti di integrabilità, facilità nell'interrogazione, capacità di rappresentazione delle informazioni. ► **WpDataTables ®**: rappresenta un componente di Data Visualization, per l'analisi e la rappresentazione di Basi Dati (anche di grandi dimensioni); garantisce semplicità di utilizzo (grazie al sistema "drag & drop") e la possibilità di esplorare "in profondità" i dati, rappresentarli in modo efficace attraverso il supporto grafico e condividerli in modo interattivo.



Il sistema di reporting configurato è stato selezionato dal RTI perché caratterizzato dai seguenti punti di forza: ► **facilità d'uso**: per utilizzare gli strumenti di analisi e monitoraggio proposti non occorre essere dei programmatori, grazie all'intuitivo sistema "drag & drop" caratterizzato da interfacce "user friendly"; ► **analisi di qualunque tipo di dato**: è possibile analizzare dai semplici fogli di calcolo (xlsx, csv, txt, ecc.) ai Database e strutture dati più complesse tipiche dei Big Data; ► **cruscotti interattivi**: le infinite combinazioni di "viste" interattive confermano gli strumenti proposti leader nella Data Preparation, Data Visualization e Data Story Telling; ► **dati sempre aggiornati**: è possibile "connettersi" a diversi sistemi e fonti dati, scegliendo la modalità di aggiornamento (automatica, pianificata, manuale); ► **condivisione interattiva**: in pochi click è possibile pubblicare e condividere le proprie analisi sul web, mantenendo sempre l'interattività dei dati.

10.2 Soluzioni, processi, strumenti di comunicazione e di collaborazione in chiave "social" con le PA contraenti

In coerenza con l'approccio proposto dal RTI che si rifà all'adozione di tecnologie digitali per stimolare la comunicazione in chiave "social" e innescare nuove modalità di lavoro collaborative (anche attraverso la creazione di spazi di co-working), il Portale prevederà alcuni moduli di collaboration. La soluzione

tecnologica identificata a supporto è la piattaforma **Open2.0®**,è un software open source la creazione di piattaforme software complesse e strumenti collaborativi che ha ottenuto tra l'altro la qualificazione di AgID come software a riuso per la Pubblica Amministrazione.

L'utente PA "accreditato", una volta effettuato il log-in, visualizzerà una Home Page personalizzata che lo abiliterà ad interagire con i "colleghi" delle altre Amministrazioni. Il Portale prevede tre soluzioni di collaboration che coprono rispettivamente: **l'anima social con una bacheca pubblica per la PA, l'anima di collaboration con una community in costante aggiornamento, gli spazi di co-working.**

La Bacheca di discussione pubblica delle PA

Uno "spazio virtuale" aperto dove poter pubblicare notizie, richiedere informazioni e/o abilitare gli altri utenti a commentare e caricare allegati a beneficio esteso di tutta la community della PA. La Bacheca riprende il concept oramai largamente diffuso dei principali strumenti social di maggior successo commerciale (i.e. Linkedin, Facebook, ecc.). In quest'area i contenuti saranno più "statici"; saranno infatti le rispettive Amministrazioni a valutare e decidere quali articoli, dati, informazioni, risultati dovranno essere esposti. L'interazione sarà "mediata" da un processo di moderazione dei post e dei commenti; tramite questo "spazio", le Amministrazioni possono "fare rete" e creare una base di conoscenza condivisa, soprattutto per quelle PA che collaborano in territori con caratteristiche simili e/o con la stessa tipologia di utenza, così da ridurre la complessità ed aumentare l'efficacia dell'azione amministrativa.

La Community di divulgazione delle esperienze

Uno spazio che ha l'obiettivo di condividere con gli utenti interessati i dettagli delle singole esperienze/iniziative progettuali maturate. Questo modulo si configura come un "catalogo delle esperienze", etichettate per tipologia di servizio e per stato (appena avviata, in corso di svolgimento, terminata), allo scopo di abilitare una rapida ricerca in base alle specifiche preferenze dell'utenza. Gli utenti avranno la possibilità di manifestare la propria preferenza per la singola esperienza: questa funzionalità permetterà al sistema di portare automaticamente "in primo piano" le iniziative più "quotate". Le esperienze sono valorizzate con la pubblicazione di una pagina di dettaglio, nella quale si possono reperire i contatti dei referenti di progetto, inserire commenti e/o allegare documentazione rilevante.

Gli spazi riservati di co-working

Il terzo modulo si configura come lo spazio di collaborazione che risponde all'esigenza di maggior privacy nella condivisione delle informazioni e del know-how acquisito nell'ambito delle progettualità avviate all'interno dell'Accordo Quadro. Gli spazi riservati di co-working potranno essere creati o a partire dalla "Community di divulgazione delle esperienze" (attraverso un'apposita funzionalità di richiesta di collaborazione all'interno della pagina di dettaglio) oppure "ex novo" (slegati quindi da specifiche esperienze maturate dalle PA). Il RTI, a fronte di analisi di benchmark effettuate per Enti Pubblici in ambito di tool di collaboration, prevede anche l'inserimento di un modulo di "team matching", strumento indispensabile per la ricerca di collaborazioni.

Il RTI si assume la responsabilità di garantire tutti gli obblighi contenuti a pag. 41 del punto 9.1 del Capitolato Tecnico Generale.

11 Miglioramento soglie indicatori di qualità: RLFN – Rilievi sulla fornitura

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico Speciale "Indicatori di qualità", il RTI si impegna a garantire una riduzione della soglia dell'indicatore **RLFN - Rilievi sulla fornitura** ad un valore pari a 1.

12 Miglioramento soglie indicatori di qualità: SLSC – Rispetto di una scadenza contrattuale

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico Speciale "Indicatori di qualità", il RTI si impegna a garantire una riduzione della soglia dell'indicatore **SLSC - Rispetto di una scadenza contrattuale** ad un valore pari a 1.

13 Miglioramento soglie indicatori di qualità: NAPP – Non approvazione di documenti

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico Speciale "Indicatori di qualità", il RTI si impegna a garantire una riduzione della soglia dell'indicatore **NAPP - Non approvazione di documenti** ad un valore pari a 0.

14 Innovazione

"L'innovazione consiste nel vedere ciò che tutti hanno visto e nel pensare ciò che nessuno ha pensato"
(Albert Szent-Gyorgyi)

Il coinvolgimento delle PMI e dei Centri di ricerca **avviene a livello di RTI** al fine di garantire la massima rapidità nell'attivazione e nel coinvolgimento di tali operatori specializzati; il ruolo di questi soggetti è duplice: **a) operare da centri di competenza per il supporto orizzontale alla erogazione dei servizi del Lotto**, fornendo spunti metodologici, best practices, strumenti e professionalità disponibili per tutti gli stakeholders; **b) operare direttamente nella erogazione di servizi** a favore di specifiche PA a causa di specificità geografiche favorevoli e/o opportunità di impiego di competenze specialistiche della PMI. Come evidenziato nella tabella **disponiamo di strutture in grado di favorire innovazione per ognuno dei servizi della presente fornitura.**

14.1 Soggetti coinvolti, principali caratteristiche e valore aggiunto

PMI/Start up innovativa	Caratteristiche	Ambito di intervento	Valore aggiunto per l'esecuzione delle prestazioni
Teleconsys Sharing Innovation	Teleconsys ha specifiche competenze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection e Intelligence. Inoltre, è fondatore e socio Gold del Digital Innovation Hub del Lazio; fa parte del board della Sezione IT di Unindustria ed è membro del Tavolo Tecnico Università, Ricerca e Trasferimento Tecnologico che lavora con le sette università del Lazio per il trasferimento tecnologico e la promozione dell'Open Innovation.	- Vulnerability Assessment - Security Strategy - Testing codice - Penetration Test.	- Fornisce una piattaforma innovativa che, abbracciando il paradigma della API Economy, è finalizzata a dare maggior valore alla compliance normativa e fornire uno strumento a servizio dell'analisi e gestione degli incidenti in ambito cybersecurity sfruttando strumenti innovativi di AI e Deep Learning. - Offre, grazie ad uno specialistico network, un ampliamento delle competenze funzionali, metodologiche e tecnologiche, nonché un supporto specializzato su trend e soluzioni emergenti in ambito cybersecurity.

Centri di ricerca	Società/Istituto	Caratteristiche	Ambito di intervento	Valore aggiunto per l'esecuzione delle prestazioni
Cyber Security Vulnerability Research Center	intellera consulting	Centro di ricerca specializzato nell'individuazione di vulnerabilità non note su sistemi e prodotti.	- Vulnerability Assessment - Penetration test	- Consente l'individuazione di vulnerabilità di tipo zero-day, fornendo dei workaround per la gestione delle stesse prima ancora che vengano rilasciate patch ufficiali dai vendor
Cyber Security Threat Intelligence Research Center	intellera consulting	Centro di ricerca specializzato nella definizione di strategie innovative per la risposta agli incidenti attraverso analisi degli strumenti di mercato e di malware analysis.	- Supporto all'analisi e gestione degli incidenti	- Definisce modalità di risposta verso delle minacce non ancora note o diffuse nel panorama mondiale e di preparare i clienti ad affrontarle. - Guida il cliente all'identificazione delle migliori soluzioni software per le loro esigenze.
Cybersecurity Experience Center	Capgemini	Centro di ricerca che nasce con l'obiettivo di supportare i clienti a prevenire gli incidenti informatici e a ridurre l'impatto di attacchi significativi.	- Supporto all'analisi e gestione degli incidenti - Vulnerability Assessment - Testing Del Codice	- Offre una simulazione immersiva per un supporto nella comprensione delle dinamiche di un incidente di sicurezza informatica e la tecnologia, le persone e i processi necessari per proteggere il core business.
Information Security Governance	TXT HSPI	Centro di ricerca specializzato nell'analisi di processi e assetti organizzativi per identificare obiettivi e strategie in ambito cybersecurity coerenti con i contesti di mercato ed aderenti alle normative vigenti.	- Security strategy - Compliance normativa	Il centro di competenza assicura il continuo approfondimento e contestualizzazione di standard e linee guida internazionali in materia di Governance della sicurezza delle informazioni.

14.2 Modalità organizzative del coinvolgimento, in termini sia di tempistiche di ingaggio, che di modalità di relazione internamente e verso le Amministrazioni

Per assicurare un continuo e qualificato supporto di innovazione alla realizzazione dei servizi di fornitura abbiamo definito una **modalità di coinvolgimento ed interazione con le Amministrazioni** basato su tre pilastri: ► *Azzeramento delle tempistiche di attivazione*, grazie alla disponibilità di tutte le competenze necessarie già all'interno del Raggruppamento. ► *Presidio continuo delle esigenze delle Amministrazioni*, attraverso figure chiavi quali l'Account Manager e il Knowledge Manager, coordinati centralmente dallo SPESI al fine di facilitare la distribuzione della conoscenza e permettere il riutilizzo di soluzioni tra differenti Amministrazioni che risultino simili per contesto ed esigenze. ► *Analisi continua e specializzata dei principali trend di innovazione* da parte dei centri di ricerca e dei relativi network che garantisca proattività e rapidità nel cogliere le evoluzioni del mercato e trasformale in soluzioni per le Amministrazioni grazie all'esperienza e al modello organizzativo flessibile del **Security & Privacy Enabler Solution Innovators (SPESI).**

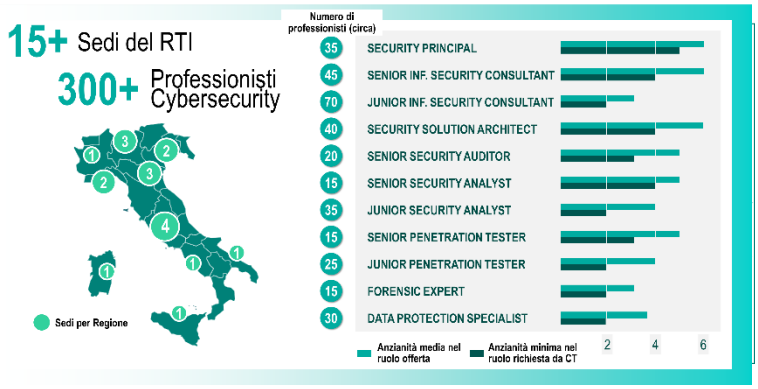
15 Flessibilità delle risorse

Sii saldo nelle tue decisioni ma rimani flessibile nel tuo approccio (Tony Robbins)

In uno scenario caratterizzato dalla necessità di staffing continuo di risorse specialistiche su numerosi Contratti Esecutivi attivabili in parallelo, è fondamentale dotarsi di un efficace processo di **workforce management** che assicuri, da un lato, la gestione integrata e multilivello del miglior mix quali-quantitativo delle risorse specialistiche, e dall'altro, tempi di disponibilità brevi o a volte brevissimi, come ad esempio la gestione di incidenti potenzialmente ad alto impatto dirompente sui sistemi delle Amministrazioni.

15.1 Disponibilità e tempestività di allocazione delle risorse in relazione all'ambito di riferimento del Lotto

Grazie alla consolidata esperienza delle nostre aziende sui temi della presente fornitura, disponiamo di **oltre 300** risorse in ambito Cyber Security (con **anzianità media nel ruolo superiore e certificazioni aggiuntive** rispetto ai requisiti minimi richiesti nell'*Appendice 2 al CTS Lotto 2_Profili Professionali)*, utilmente impiegabili ed **opportunamente distribuite territorialmente.** Le nostre aziende dispongono di forti legami di partnership con i più diffusi e importanti vendor tecnologici che garantiscono il massimo presidio verticale di competenza anche sui prodotti e soluzioni di mercato. **La rete di partnership del RTI permette di coprire tutti i servizi richiesti nel Capitolato.**



Vista la strategicità della presente fornitura, intendiamo adottare ogni soluzione a nostra disposizione per garantire **piena e immediata impiegabilità di tutta la capacità produttiva disponibile**. In particolare, faremo ricorso a: ► **Processi** di pre-booking delle risorse dei nostri centri di competenze e delivery sui diversi contratti esecutivi potenzialmente attivabili, in base ad analisi di tendenza, confronti tecnico-commerciali con le Amministrazioni interessate, demand management, ecc.; ► **Team di twin resources**: per le risorse chiave identificate nell'ambito dell'AQ sarà identificato un pool di risorse aggiuntive, con competenze interscambiabili, da allocare sulle attività critiche ad integrazione delle risorse dei team. Tale soluzione consentirà di assicurare l'immediato allineamento della forza lavoro e delle competenze alle variazioni sia in incremento dell'effort, sia in caso di indisponibilità temporanea, senza alcun onere aggiuntivo e/o disservizio per la Committenza. Per garantire risorse immediatamente attivabili, i professionisti del pool di risorse aggiuntive saranno continuamente allineati sul contratto e sulle attività attraverso workshop tematici. I workshop riguardano, in primis: ① **aggiornamenti su forniture tra le più complesse e ritenute "a più alto grado di variabilità",** ② aggiornamenti sull'evoluzione dei contratti nell'ambito dell'AQ. Ai workshop si aggiunge il processo di formazione continua (cfr. *§ 16 Aggiornamento delle risorse professionali*); ► **Team di continuità**: per i servizi che nel corso della fornitura dovessero subire sospensioni temporanee e/o riduzioni di effort, in caso di ripresa/incremento delle relative attività, assicureremo la riallocazione delle medesime risorse che precedentemente operavano nell'ambito degli stessi, a garanzia di abbattimento dei tempi di ingaggio sul singolo intervento e salvaguardia del know-how; ► **Orario flessibile**: fermo restando il pieno rispetto degli orari di lavoro previsti dai contratti, le risorse impegnate sui singoli task progettuali potranno essere allocate secondo una logica di turnazione per coprire una fascia oraria giornaliera di lavoro più ampia (es. dalle 8.00 alle 20.00) rispetto a quella indicata nel Capitolato (cfr. § 5.9 Orario di erogazione dei servizi). Tale misura consentirà un presidio continuativo più ampio rispetto alle normali otto ore di lavoro e garantirà una più efficace operatività in relazione ad attività critiche. In casi di particolare emergenza in cui si renda necessario concentrare in tempo reale forza lavoro (es. per far fronte a improvvise/coincidenti scadenze) potrà, inoltre, essere fatto ricorso al lavoro straordinario.

La presente fornitura contiene linee di servizio nelle quali la **tempestività** è, nei fatti, uno dei fattori critici di successo (es. nel caso della gestione degli incidenti informatici). Per ottimizzare i tempi di risposta al riguardo, il RTI attiva tutte le leve di disponibilità sopra illustrate in tempi estremamente rapidi grazie a: ► **la presenza di presidi organizzativi** deputati ad **intercettare in tempi ridotti** (e dove possibile anticipare) le esigenze dei clienti o potenziali clienti (processo di demand management opportunamente presidiato da Demand Manager specifici per ogni Contratto); a **valutare in anticipo esigenze di modifiche di staffing** dovute ad emergenze o criticità particolari (Project Risk Management) o a modifiche nella pianificazione (PMO); a **presidiare con piena e diretta responsabilità i processi di staffing** (Resource Manager); ► **l'utilizzo di strumenti integrati di workforce management e di skill inventory** (es. Talent Link) di supporto alla pianificazione e rimodulazione delle risorse specialistiche.

Grazie a queste soluzioni il RTI è in grado di mettere a disposizione delle Amministrazioni un team di risorse specialistiche, per ciascuno dei servizi previsti, **al di fuori della pianificazione prevista nel Piano di Lavoro Generale**, con le seguenti tempistiche: ► **entro 3 giorni dall'esigenza** per i servizi di "Security Strategy", "Vulnerability Assessment", "Testing del codice (Statico, Dinamico o Mobile)", "Penetration Testing" e "Compliance Normativa"; ► **entro 3 ore dalla esigenza,** per il servizio di "Supporto analisi e gestione incidenti".

15.2 Metodologie e strumenti proposti per la flessibilità nella gestione di più contratti in contemporanea

Per garantire flessibilità nella gestione di progetti in contemporanea adottiamo un **framework di Agile Program Management** (*cfr. § 3* Struttura Organizzativa), strutturato in metodologie di dettaglio e strumenti che rappresentano best *practice* di Scaled Agile applicate allo specifico contesto della fornitura. Questa metodologia agile garantisce un **coordinamento e controllo complessivo di tutte le iniziative progettuali** che verranno attivate e, allo stesso modo la necessaria flessibilità e tempestività d'azione necessarie alla gestione contemporanea di più progetti (sia presso la stessa Amministrazione che in più Amministrazioni). A livello di Accordo Quadro, in particolare, grazie alle metodologie di **Portfolio, Program e Team backlog management** siamo in grado di aggregare e disaggregare le iniziative legandole ad attività sempre più granulari che consentono un **controllo più efficace ed una maggiore adattabilità e flessibilità in caso di cambiamenti,** indipendentemente dal livello (inter-Amministrazioni o intra-Amministrazione). A livello esecutivo progettuale, invece, grazie all'**approccio incrementale** basato su **metodologie agile** anticipiamo il risultato finale e garantiamo flessibilità e tempestività soprattutto nel raccogliere i feedback delle Amministrazioni mitigando i rischi e massimizzando così l'efficacia del risultato finale della delivery. Nel dettaglio grazie a metodologie operative e strumenti di **Continuous delivery** e **Sprint planning,** siamo in grado di gestire flessibilmente e tempestivamente eventuali cambiamenti e modifiche con minimizzazione degli impatti di pianificazione.

Il framework metodologico appena presentato è supportato inoltre da **strumenti** ad hoc che garantiscono: ► *Efficacia*: **Redmine** è uno strumento di Agile PPM che fornisce in modo efficiente e collaborativo, in tempo reale, analisi ed approfondimenti sulla delivery. La piattaforma digitale viene utilizzata come "fonte di verità" centralizzata per tutte le informazioni su Portafogli e Programmi, eliminando la necessità di fare affidamento su documenti e strumenti stand-alone. ► *Tempestività e Flessibilità*: **Talent Link** e **Smart Planner**: strumenti che consentono di avere una visione di insieme ed in tempo reale di tutte le skill e le competenze messe a disposizione della fornitura da parte del RTI con informazioni sempre aggiornate della percentuale di impegno

sui diversi progetti presso le diverse o le stesse Amministrazioni. Sulla base delle percentuali di ingaggio e della criticità della singola risorsa è possibile adattare in modo flessibili le composizioni dei team a picchi di lavoro, esigenze particolari ed estemporanee.

Redmine fornisce un ambiente altamente configurabile per stabilire una visione personalizzata del proprio portafoglio, consentendo a tutti gli stakeholder del progetto, del programma e del portafoglio di ottenere informazioni dettagliate sugli avanzamenti progettuali, attraverso un'interfaccia moderna e *user-friendly* che **consente un efficace gestione dei team di programma** attraverso le funzionalità mostrate nella figura seguente.

Talent Link® è la piattaforma di gestione del personale, già in uso presso le aziende del RTI, per consentire l'allocazione di risorse e competenze in risposta a una o più richieste di adesione all'AQ. L'utilizzo della piattaforma consente di identificare e selezionare le risorse ottimali sulla base delle competenze possedute e della loro disponibilità secondo una struttura a matrice che incrocia i settori di mercato a livello "verticale", (PAC, PAL, Sanità) e le aree/dominii di competenza del personale a livello "orizzontale" (Strategy, Management, Technology e Risk Consulting, ecc.). La presenza di ulteriori dati strutturati (e. le esperienze avute, i clienti per i quali hanno lavorato, le Industry conosciute, ecc.) consente di valutarne l'utilizzabilità per la fornitura con **ricerche mirate e su più criteri**. Talent link è integrato con lo strumento **Smart Planner®**, utilizzato dal RTI per la **gestione della pianificazione** delle persone. Permette di visualizzare l'impegno di una risorsa mappandone il progetto e il cliente per cui sta lavorando. Tali strumenti consentono la simulazione, il planning giornaliero, la valutazione delle competenze e delle performance del personale impiegato, la **gap analysis** di competenze e risorse nei team e le necessarie azioni correttive.

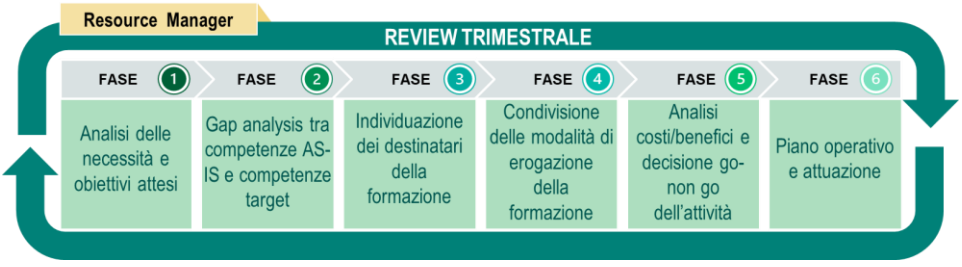
16 Aggiornamento delle risorse professionali

La peculiarità dei servizi di gara richiede il presidio di frontiere di conoscenza tematiche (normative, studi di settore, best practice) e tecnologiche (prodotti, tecniche, strumenti specifici) da preservare nel tempo con **metodi e programmi di formazione diversificati per figura professionale**. I numeri di seguito testimoniano l'impegno che il RTI dedica alle attività formative: ① **Oltre 7 giorni medi per risorsa dedicati ogni anno ad attività formative**, di cui **4 riservati all'IT Security**; ② **Oltre 1.500 certificazioni** tecnologiche e metodologiche, di cui **oltre 250 in ambito IT Security**; ③ Disponibilità di **oltre 10 docenti accreditati** ad erogare formazione certificata di cui **2 in ambito IT Security**.

16.1 Soluzioni progettuali e strumenti tecnologici per garantire la formazione e l'aggiornamento continuo

La formazione e l'aggiornamento continuo delle risorse impiegate nella fornitura sono garantite - senza alcun onere aggiuntivo per le Amministrazioni - da un **framework formativo** che ha le seguenti caratteristiche: una soluzione organizzativa snella ed efficace, un processo specifico a supporto, contenuti e modalità di erogazione differenziate e soggette a review periodiche, uno strumento in grado di gestire e tracciare tutte le attività di formazione.

La **soluzione organizzativa** prevede: ① un **Resource Manager** a livello di intero Accordo Quadro, che supervisiona l'intero processo di framework formativo, fornisce supporto metodologico per la standardizzazione delle modalità formative, mantenendo uno skill inventory centralizzato ed aggiornato; ② **professionisti con esperienza certificata sui temi della formazione** nei team di progetto a livello di contratto esecutivo, per individuare e pianificare le esigenze formative specifiche legate ai servizi offerti nel contratto.



Un **processo formativo**, basato su sei fasi e schematizzato in figura, per garantire concretezza ed efficacia rispetto alle continue evoluzioni del mercato. Un **mix di metodologie elementari** che assicurano il raggiungimento degli obiettivi di efficacia del piano formativo:

- **Lezione frontale**, consente di acquisire nozioni teoriche e di attivare confronti tra discenti
- **Laboratori/esercitazioni**, le esercitazioni pratiche assicurano un adeguato bilanciamento tra teoria e pratica
- **Simulazioni/Role-Playing**: basata sulla immaginazione e capacità di immedesimazione in una determinata situazione
- **Risorse online**: corsi e-learning per la fruizione asincrona sulla piattaforma **Moodle**
- **Gamification**: metodologia asincrona nella quale i discenti sono coinvolti in una serie di processi e pratiche proprie del gioco.
- **Sessioni di Studio/Eventi**: workshop organizzati da organizzazioni nazionali/internazionali per promuovere specifici eventi tematici

Uno **strumento tecnologico** denominato ILMS (*Intellera Learning Management System)* che integra sulla piattaforma Moodle tutte le features di un Learning Management System consentendo la gestione completamente digitalizzata del processo sopra-descritto a partire dalla analisi del fabbisogno, fino alla erogazione del corso e alla certificazione di avvenuta acquisizione delle competenze correlate. Lo strumento è nativamente integrato con Talent

Link - lo strumento di tracciatura delle competenze del personale (cfr. 15.2 Metodologie e strumenti proposti per la flessibilità nella gestione di più contratti in contemporanea) - ed è reso accessibile sia in modalità web che mobile a tutto il personale coinvolto nella presente fornitura.

16.2 Completezza ed efficacia della proposta di piano formativo

Il tailoring specifico del framework sui contenuti del piano formativo si basa su tre direttrici: ① **Mantenimento ed integrazione delle certificazioni** previste dai profili e migliorate in fase di Offerta Tecnica; ② **Sensibilizzazione rispetto alla sicurezza nell'erogazione dei servizi**; ③ **Aggiornamento su standard e normative**. I corsi **in ambito IT Security** identificati sono i seguenti:

Ambito	Cluster Formativi	Figura Professionale / Ore anno										
		SP	SISC	JISC	SSAR	SSAU	SSA	JSA	SPT	JPT	FE	DPS
Sensibiliz-zazione	Uso dotazioni informatiche in tutte le modalità operative (meccanismi e regole definite per la protezione dei dati che verranno acquisiti nel corso delle operazioni). Formazione su regole, procedure, SLA previsti dall'AQ. Formazione sugli standard definiti per i deliverable di progetto	8	8	8	8	8	8	8	8	8	8	8
Governance, Risk and Control	CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk & Information Systems Control), CISSP (Certified Information Systems Security Professional), ISO/IEC 27001, COBIT, CMMI.	32				32						16
Normative	CDPSE (Certified Data Privacy Solution Engineer). ISO/IEC 27701/27017/27018. Gestione data breach, GDPR e misure di sicurezza, Analisi rischi e valutazioni di impatto, Registro dei trattamenti. Aggiornamento normative privacy, ecc.	8	24	24	8	16	8	16				32
Technical Skills 1	EC-Council CSA (Certified Ethical Hacker), EC-Council CSA (Certified SOC Analyst), CompTIA CySA+ (Cyber Security Analyst), OSSTMM Professional Security Tester, GIAC CFA/CFE/DFIP/CIH/ENCE						32		32	16	32	
Technical Skills 2	Prodotti di sicurezza (FW, Antimalware, IDS/IPS, WAF, SIEM, I&AM, ecc.) Architetture, protocolli e servizi infrastrutturali. Processi di hardening di sistemi s middleware. Sviluppo sicuro del codice. Sicurezza architetture di Cloud Computing		24	24	40		8	24	24	32	24	
P&S Mgmt	ITIL, Prince2, PMI	8					8	8				
Framework di Controllo	Eventi CSA (Cloud Security Alliance), Aggiornamento principali framework di controlli: NIST cybersecurity framework e framework nazionale, CSA-CCM, CIS-CSC (ex SANS20), Linee guida AGID (e nuova Agenzia), Linee guida ENISA	8	8	8	8	8		8		8		8

Al fine di evitare impatti della formazione sull'erogazione dei servizi si agirà sui seguenti aspetti: ► privilegio della modalità e-learning da fruire di norma al di fuori del normale orario di lavoro (utilizzo del regime dello straordinario); ► pianificazione organizzata per non impegnare nella stessa sessione un numero sostenuto di risorse del medesimo profilo e/o che operano nel medesimo team operativo; ► in caso di sessione formativa che richiede la "presenza fisica" dei discenti in aula, le risorse allocate stabilmente sui servizi potranno essere sostituite, qualora necessario, da risorse del pool di risorse ausiliarie. Per consentire una **gestione integrata e un monitoraggio qualitativo e quantitativo sull'andamento delle iniziative formative** declinate nel Piano di Formazione, sarà messa a disposizione una dashboard ad uso del livello Governo, all'interno del Portale di Governo della Fornitura, con appositi **report e viste informative multidimensionali** al fine di dare evidenza alle Amministrazioni, ed a Consip, delle iniziative formative effettuate e previste.

17 Assunzione delle risorse professionali

Rispetto al complesso delle assunzioni necessarie per ogni contratto esecutivo finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, e fermo restando il rispetto del requisito necessario di cui al Capitolato tecnico generale al par. 7.1, il RTI si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, almeno nella misura del 36%.

18 Documentazione coperta da riservatezza

L'opposizione all'ostensione è motivata in ragione del presupposto che l'Offerta Tecnica contiene informazioni di carattere estremamente riservato, riguardanti il *know-how* e, in particolare, le metodologie e gli strumenti che caratterizzano il servizio offerto dallo Scrivente RTI, nonché le strategie tecniche e commerciali seguite dalle Società. Informazioni che, ove rese note alle società concorrenti, nuocerebbero gravemente agli interessi commerciali e imprenditoriali dello Scrivente RTI, con conseguente inevitabile pregiudizio di ogni futuro leale confronto concorrenziale. Per i motivi sopra esposti, pertanto, si chiede a codesta Amministrazione di non consentire l'accesso, sia con riferimento alla visione sia all'estrazione di copia, degli atti e parti di atti di cui sopra, per ragioni inerenti alla tutela dei diritti di privativa commerciale di titolarità dello Scrivente RTI.

intellera consulting — **Giancarlo Senatore – Mario Papini**

Capgemini — **Andrea Falleni**

TXT HSPI — **Sebastiano Manno**

Teleconsys Sharing Innovation — **Giada Apicella**

ALLEGATO B – OFFERTA ECONOMICA DEL FORNITORE

acquistinretepa.it
Il Portale degli acquisti della Pubblica Amministrazione

Offerta economica relativa a:	
Numero Gara	2860180
Nome Gara	Gara a procedura aperta per la conclusione di un Accordo Quadro ai sensi del D.Lgs. 50/2016 e s.m.i., suddivisa in due lotti, avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296
Criterio di Aggiudicazione	Gara ad offerta economicamente più vantaggiosa
Lotto	1 (Servizi di compliance e controllo)

AMMINISTRAZIONE TITOLARE DEL PROCEDIMENTO	
Amministrazione	CONSIP SPA
Partita IVA	05359681003
Indirizzo	VIA ISONZO 19/E - ROMA (RM)

CONCORRENTE	
Forma di Partecipazione	R.T.I. costituendo (D.Lgs. 50/2016, art. 48, comma 8)
Ragione Sociale	INTELLERA CONSULTING (mandataria) Società a Responsabilità Limitata
Partita IVA	11088550964
Codice Fiscale Impresa	11088550964
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	11088550964
Codice Ditta INAIL	20521450 cc 52 -
n. P.A.T.	95768199 cc 28 - PAT2 95768500 cc 31
Matricola aziendale INPS	4989063256
CCNL applicato	TERZIARIO - INDUSTRIA
Settore	CONSULENZA
Indirizzo sede legale	PIAZZA TRE TORRI N. 2 - MILANO (MI)

Telefono	06570832136
Fax	0657822536
PEC Registro Imprese	INTELLERA@PEC-INTELLERACONSULTING.COM
Ragione Sociale	CAPGEMINI ITALIA S.P.A. (mandante) Società per Azioni
Partita IVA	04877961005
Codice Fiscale Impresa	10365640159
Provincia sede registro imprese	RM
Numero iscrizione registro imprese	10365640159
Codice Ditta INAIL	05701878 81
n. P.A.T.	10468727 73;10468870 60;10468868 97
Matricola aziendale INPS	7037550355 09
CCNL applicato	INDUSTRIA METALMECCANICA E DELLA INSTALLAZIONE DI IMPIANTI
Settore	METALMECCANICO
Indirizzo sede legale	VIA DI TORRE SPACCATA, 140 - ROMA (RM)
Telefono	06231901
Fax	062382777
PEC Registro Imprese	GARE@PEC.CAPGEMINI.IT
Ragione Sociale	HSPI SPA (mandante) Società per Azioni
Partita IVA	02355801206
Codice Fiscale Impresa	02355801206
Provincia sede registro imprese	BO
Numero iscrizione registro imprese	02355801206
Codice Ditta INAIL	013681157/48 - BOLOGNA1 (18100)
n. P.A.T.	91151038/28
Matricola aziendale INPS	1314121948 UNICO - BOLOGNA (1300)
CCNL applicato	TERZIARIO
Settore	SERVIZI
Indirizzo sede legale	VIA ALDO MORO, 16 - BOLOGNA (BO)
Telefono	3484527615
Fax	06874598794
PEC Registro Imprese	PEC.HSPI@PEC.IT
Ragione Sociale	TELECONSYS (mandante) Società per Azioni
Partita IVA	07059981006
Codice Fiscale Impresa	07059981006
Provincia sede registro imprese	RM
Numero iscrizione registro imprese	07059981006

Codice Ditta INAIL	0013538002-46
n. P.A.T.	90938255/79-72
Matricola aziendale INPS	7046855445
CCNL applicato	COMMERCIO
Settore	SETTORE DELLE TELECOMUNICAZIONI, DELL' INFORMATICA, DELLA TELEMATICA E DEI SISTEMI ELETTRICI, OTTICI, MECCANICI E MECCATRONICI IN GENERALE AD ESSA FUNZIONALI
Indirizzo sede legale	VIA GROENLANDIA 31 - ROMA (RM)
Telefono	0620396767
Fax	0620396768
PEC Registro Imprese	TELECONSYS.MAIL@POSTECERT.IT
Offerta sottoscritta da	**APICELLA GIADA, SENATORE GIANCARLO, PAPINI MARIO, MANNO SEBASTIANO, FALLENI ANDREA**

Scheda di Offerta	
Descrizione	Servizi di compliance e controllo - offerta economica
Offerta Economica	
Parametro Richiesto	**Valore Offerto**
1 - L1.S16 - Security Strategy - gg/p Team ottimale - Prezzo unitario offerto (€)	260,00
2 - L1.S17 - Vulnerability Assesssment - gg/p Team ottimale - Prezzo unitario offerto (€)	235,00
3 - L1.S18 -Testing del codice - Statica - Singola esecuzione - Prezzo unitario offerto (€)	864,50
4 - L1.S18 -Testing del codice - Statica - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	839,80
5 - L1.S18 -Testing del codice - Statica - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	810,16
6 - L1.S18 -Testing del codice - Statica - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	796,75
7 - L1.S19 - Testing del codice - Dinamica - Gold - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	2593,50
8 - - Gold - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	1971,06
9 - - Gold - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	1478,29
10 - - Silver - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	1395,83
11 - - Silver - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	1149,78
12 - - Silver - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	998,40
13 - - Bronze - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	564,20

14 - - Bronze - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	483,60
15 - - Bronze - Fascia 3- > 50 applicazioni - Prezzo unitario offerto (€)	432,25
16 - L1.S20 -Testing del codice - Mobile - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	1797,32
17 - L1.S20 -Testing del codice - Mobile - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	1654,09
18 - L1.S20 -Testing del codice - Mobile - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	1490,30
19 - L1.S21 -Supporto all’analisi e gestione degli incidenti - gg/p Team ottimale - Prezzo unitario offerto (€)	210,00
20 - L1.S22 -Penetration testing - gg/p Team ottimale - Prezzo unitario offerto (€)	256,20
21 - L1.S23 -Compliance normativa - gg/p Team ottimale - Prezzo unitario offerto (€)	200,00
Ribasso medio ponderato - Calcolato dal Sistema	0,48055

Il Concorrente, nell'accettare tutte le condizioni specificate nella documentazione del procedimento, altresì dichiara:

- che la presente offerta è irrevocabile ed impegnativa sino al termine di conclusione del procedimento, così come previsto nella lex specialis;
- che la presente offerta non vincolerà in alcun modo la Stazione Appaltante/Ente Committente;
- di aver preso visione ed incondizionata accettazione delle clausole e condizioni riportate nel Capitolato Tecnico e nella documentazione di Gara, nonché di quanto contenuto nel Capitolato d'oneri/Disciplinare di gara e, comunque, di aver preso cognizione di tutte le circostanze generali e speciali che possono interessare l'esecuzione di tutte le prestazioni oggetto del Contratto e che di tali circostanze ha tenuto conto nella determinazione dei prezzi richiesti e offerti, ritenuti remunerativi;
- di non eccepire, durante l'esecuzione del Contratto, la mancata conoscenza di condizioni o la sopravvenienza di elementi non valutati o non considerati, salvo che tali elementi si configurino come cause di forza maggiore contemplate dal codice civile e non escluse da altre norme di legge e/o dalla documentazione di gara;
- che i prezzi/sconti offerti sono omnicomprensivi di quanto previsto negli atti di gara;
- che i termini stabiliti nel Contratto e/o nel Capitolato Tecnico relativi ai tempi di esecuzione delle prestazioni sono da considerarsi a tutti gli effetti termini essenziali ai sensi e per gli effetti dell'articolo 1457 cod. civ.;
- che il Capitolato Tecnico, così come gli altri atti di gara, ivi compreso quanto stabilito relativamente alle modalità di esecuzione contrattuali, costituiranno parte integrante e sostanziale del contratto che verrà stipulato con la stazione appaltante/ente committente.

ATTENZIONE: QUESTO DOCUMENTO NON HA VALORE SE PRIVO DELLA SOTTOSCRIZIONE A MEZZO FIRMA DIGITALE

ALLEGATO C – CORRISPETTIVI E TARIFFE PAC

ACCORDO QUADRO PER L'AFFIDAMENTO SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI AI SENSI DELL'ART. ex art. 54, co. 4 lett. a) DEL d.lgs. N. 50/2016 – ID 2296

Lotto 2 - Servizi di compliance e controllo per le Pubbliche Amministrazioni Centrali (PAC)

Servizio	Id.	Voce economica	Prezzo offerto
L1.S16 - Security Strategy	1	gg/p Team ottimale	€ 260,00
L1.S17 - Vulnerability Assesssment	2	gg/p Team ottimale	€ 235,00
L1.S18 -Testing del codice - Statica	3	Singola esecuzione	€ 864,50
	4	Fascia 1 - Fino a 15 applicazioni	€ 839,80
	5	Fascia 2 - Fino a 50 applicazioni	€ 810,16
	6	Fascia 3 - > 50 applicazioni	€ 796,75
L1.S19 - Testing del codice - Dinamica	7	Gold - Fascia 1 - Fino a 15 applicazioni	€ 2.593,50
	8	Gold - Fascia 2 - Fino a 50 applicazioni	€ 1.971,06
	9	Gold - Fascia 3 - > 50 applicazioni	€ 1.478,29
	10	Silver - Fascia 1 - Fino a 15 applicazioni	€ 1.395,83
	11	Silver - Fascia 2 - Fino a 50 applicazioni	€ 1.149,78
	12	Silver - Fascia 3 - > 50 applicazioni	€ 998,40
	13	Bronze - Fascia 1 - Fino a 15 applicazioni	€ 564,20
	14	Bronze - Fascia 2 - Fino a 50 applicazioni	€ 483,60
	15	Bronze - Fascia 3- > 50 applicazioni	€ 432,25
L1.S20 -Testing del codice - Mobile	16	Fascia 1 - Fino a 15 applicazioni	€ 1.797,32
	17	Fascia 2 - Fino a 50 applicazioni	€ 1.654,09
	18	Fascia 3 - > 50 applicazioni	€ 1.490,30

L1.S21 -Supporto all'analisi e gestione degli incidenti	19	gg/p Team ottimale	€ 210,00
L1.S22 -Penetration testing	20	gg/p Team ottimale	€ 256,20
L1.S23 -Compliance normativa	21	gg/p Team ottimale	€ 200,00

ALLEGATO D – PATTO D'INTEGRITA'

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

PATTO DI INTEGRITA' RELATIVO ALLA PROCEDURA DI GARA 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

LOTTO 2

ALLEGATO D
PATTO DI INTEGRITA' AI SENSI DELLA L. 190/2012

SOMMARIO

PREMESSA

L'art. 1, comma 17 della L. 6 novembre 2012, n. 190 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione") dispone che "*le stazioni appaltanti possono prevedere negli avvisi, bandi di gara o lettere di invito che il mancato rispetto delle clausole contenute nei protocolli di legalità o nei patti di integrità costituisce causa di esclusione dalla gara*".

Il Piano Nazionale Anticorruzione, approvato con delibera n. 72/2013 dall'Autorità Nazionale Anticorruzione e successivamente aggiornato, prevede che le pubbliche amministrazioni e le stazioni appaltanti, in attuazione del citato art. 1, comma 17 della L. 190/2012, predispongono e utilizzano protocolli di legalità o patti di integrità per l'affidamento di appalti pubblici. A tal fine, i predetti soggetti inseriscono negli avvisi, nei bandi di gara e nelle lettere di invito la clausola di salvaguardia che il mancato rispetto del protocollo di legalità o del patto di integrità dà luogo all'esclusione dalla gara e alla risoluzione del contratto.

L'ANAC, inoltre, con il parere 11/2014, si è espressa favorevolmente riguardo alla previsione del bando che richiede l'accettazione dei protocolli di legalità e dei patti di integrità quale possibile causa di esclusione, *"in quanto tali mezzi sono posti a tutela di interessi di rango sovraordinato e gli obblighi in tal modo assunti discendono dall'applicazione di norme imperative di ordine pubblico, con particolare riguardo alla legislazione in materia di prevenzione e contrasto della criminalità organizzata nel settore degli appalti.".*

Infine il presente patto recepisce le raccomandazioni fornite dall'ANAC con le Linee Guida n. 15 del 12 luglio 2019.

In attuazione di quanto sopra,

SI CONVIENE QUANTO SEGUE

ART. 1 OGGETTO

1. Il presente patto di integrità (di seguito, il "**Patto di Integrità**") stabilisce la reciproca e formale obbligazione – tra

- la Consip S.p.A. a socio unico in qualità di stazione appaltante (di seguito, anche "**Consip**"),
- i soggetti legittimati, sulla base della normativa vigente, ad utilizzare l'Accordo Quadro (di seguito, anche le "**Amministrazioni**" o la "**singola Amministrazione contraente**")
- l'operatore economico partecipante alla procedura di gara (di seguito anche **il "Concorrente");**
- l'aggiudicatario della procedura di gara (di seguito, anche il "**Fornitore)** relativa alla stipula dell'Accordo Quadro ovvero dei Contratti esecutivi a valere sull'Accordo Quadro per l'affidamento dei servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni".

a conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, impegnandosi ciascuno, per quanto di rispettiva competenza, a contrastare fenomeni di corruzione e illegalità e comunque a non compiere alcun atto volto a distorcere o influenzare indebitamente il corretto svolgimento di tutte le fasi dell'appalto, dalla partecipazione alla procedura alla esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati.

2. Il Fornitore, la Consip e le Amministrazioni si impegnano a rispettare nonché a far rispettare al rispettivo personale, ai collaboratori e, per quanto riguarda il Fornitore, anche ai subappaltatori/subcontraenti/imprese ausiliarie, il presente Patto di Integrità, il cui spirito e contenuto condividono pienamente, informando gli stessi prontamente e puntualmente e vigilando scrupolosamente sulla loro osservanza.

ART. 2 AMBITO DI APPLICAZIONE

1. Il presente Patto di Integrità regola i comportamenti di tutti i soggetti individuati nel precedente art. 1, ed è vincolante:

- **per Consip S.p.A.** nella fase di espletamento della procedura di gara dell'Accordo Quadro
- **per le Amministrazioni:** nella fase di esecuzione dell'Accordo Quadro nonché nella fase di esecuzione degli Contratti esecutivi;
- **per l'Operatore Economico,** nella fase di svolgimento della procedura di gara per la stipula di Accordi Quadro e dei relativi Contratti esecutivi.
- **per il Fornitore,** nella fase di esecuzione dell'Accordo Quadro e dei Contratti esecutivi.

2. Il Patto di Integrità costituisce parte integrante e sostanziale dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati.

ART. 3 OBBLIGHI DEL CONCORRENTE E DEL FORNITORE

1. Obblighi del Concorrente:
   a1) il Concorrente s'impegna a non corrispondere né promettere di corrispondere ad alcuno – direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati - somme di denaro o altra utilità ai fini dell'aggiudicazione della gara o di distorcere il corretto svolgimento della stessa;
   b1) il Concorrente dichiara di astenersi dal compiere qualsiasi tentativo di turbativa, irregolarità o, comunque, violazione delle regole della concorrenza ovvero a segnalare tempestivamente a Consip e alla Pubblica Autorità qualsiasi tentativo di turbativa, irregolarità e violazioni delle regole di concorrenza di cui dovesse venire a conoscenza durante tutte le fasi della procedura, fornendo elementi dimostrabili a sostegno delle suddette segnalazioni;
   c1) il Concorrente si impegna a segnalare eventuali situazioni di conflitti di interesse, di cui sia o venga a conoscenza al momento della partecipazione e durante l'espletamento dell'intera procedura rispetto ai soggetti (sia di Consip che delle Amministrazioni) di cui al par. 4 delle Linee Guida Anac sopra richiamate, che siano coinvolti in una qualsiasi fase della procedura (programmazione, progettazione, preparazione documenti di gara, selezione dei concorrenti, aggiudicazione) o che possano influenzarne in qualsiasi modo l'esito in ragione del ruolo ricoperto all'interno dell'ente;
   d1) il Concorrente si impegna a far rilasciare all'impresa ausiliaria, ai fini della partecipazione alla procedura di gara, una dichiarazione di presa visione e accettazione delle clausole del presente Patto di integrità;
   e1) il Concorrente si impegna ad inserire nei contratti di avvalimento una clausola che prevede l'impegno dell'ausiliaria a rispettare gli obblighi di cui al Patto di integrità, pena la risoluzione del contratto di avvalimento e il conseguente obbligo per il Concorrente medesimo di sostituire l'impresa ausiliaria nel caso di violazione degli impegni assunti nel medesimo Patto di integrità;
   f1) il Concorrente dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A.;
2. Obblighi del Fornitore:
   a2) Il Fornitore si impegna a segnalare eventuali situazioni di conflitti di interesse, anche riferite alla fase di partecipazione alla procedura di gara, di cui sia o venga a conoscenza durante l'intera fase esecutiva del Contratto rispetto ai soggetti (sia di Consip che della Amministrazioni) di cui al par. 4 delle Linee Guida Anac sopra richiamate, che siano coinvolti in una qualsiasi fase della procedura (sottoscrizione del contratto, esecuzione, collaudo, pagamenti) o che possano influenzarne in qualsiasi modo l'esito in ragione del ruolo ricoperto all'interno dell'ente;

b2) il Fornitore dichiara di non avere influenzato il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente e di non aver corrisposto né promesso di corrispondere ad alcuno direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati - somme di denaro o altra utilità al fine di agevolare o distorcere la corretta e regolare esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati;

c2) Il Fornitore dichiara di non aver concluso con altri operatori economici alcun tipo di accordo volto ad alterare o limitare la concorrenza, ovvero a determinare un unico centro decisionale ai fini della partecipazione alla procedura di gara e della formulazione dell'offerta, risultata poi essere la migliore.

d2) Il Fornitore dichiara di astenersi dal compiere qualsiasi tentativo di turbativa, irregolarità o, comunque, violazione delle regole della concorrenza ovvero a segnalare tempestivamente a Consip, alla Pubblica Autorità e alla singola Amministrazione contraente, qualsiasi tentativo di turbativa, irregolarità e violazioni delle regole di concorrenza di cui dovesse venire a conoscenza durante la fase di esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati, fornendo elementi dimostrabili a sostegno delle suddette segnalazioni;

e2) il Fornitore si impegna a segnalare a Consip e alla singola Amministrazione contraente, nonché alla Pubblica Autorità competente e alla Prefettura, qualunque tentativo di concussione e qualsiasi illecita richiesta o pretesa da parte dei dipendenti di Consip e/-della singola Amministrazione contraente o di chiunque possa influenzare le decisioni relative all'esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente stipulati;

f2) il Fornitore si impegna ad inserire nei contratti di subappalto e negli altri subcontratti una clausola che preveda il rispetto degli obblighi di cui al presente Patto di Integrità da parte dei subappaltatori/subcontraenti, e la risoluzione, ai sensi dell'art. 1456 c.c., del contratto di subappalto, nel caso di violazione di tali obblighi da parte di questi ultimi, con conseguente comunicazione a Consip dell'avvenuta risoluzione del predetto contratto;

g2) il Fornitore di impegna a rendere noti, su richiesta dell'Amministrazione contraente, tutti i pagamenti eseguiti e riguardanti i Contratti di Fornitura e i singoli Appalti Specifici affidati;

h2) il Fornitore dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A. in relazione degli obblighi assunti dal Fornitore nei confronti di quest'ultima.

3. Il Concorrente e il Fornitore dichiarano, inoltre, di essersi già impegnati nei confronti di Consip al rispetto degli obblighi di cui al presente patto di integrità, mediante apposita dichiarazione resa in sede di partecipazione alla procedura di gara.
4. Il Concorrente e il Fornitore prendono atto ed accettano che la violazione, comunque accertata da Consip e/o dalle Amministrazioni di uno o più impegni assunti con il presente Patto di Integrità può comportare l'applicazione delle sanzioni di cui al successivo art. 5.

ART. 4 OBBLIGHI DI CONSIP E DELLE AMMINISTRAZIONI.

1. Nel rispetto del presente Patto di Integrità, Consip e le Amministrazioni si impegnano, per quanto di rispettiva competenza, a rispettare i principi di lealtà, trasparenza e correttezza di cui alla L. n. 190/2012, nonché, nel caso in cui venga riscontrata una violazione di detti principi o di prescrizioni analoghe, a valutare l'eventuale attivazione di procedimenti disciplinari nei confronti del rispettivo personale a vario titolo intervenuto nella procedura di affidamento e nell'esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi

successivamente affidati , secondo quanto previsto dai rispettivi piani di prevenzione della corruzione.

ART. 5 SANZIONI

1. Il Concorrente e il Fornitore prendono atto ed accettano che la violazione degli obblighi assunti con il presente Patto di Integrità, nonché la non veridicità delle dichiarazioni rese, comunque accertati da Consip e/o dalle Amministrazioni, può comportare l'applicazione di una o più delle seguenti sanzioni:
   a. se la violazione è accertata nella fase precedente all'aggiudicazione dell'Accordo Quadro, esclusione dalla procedura di affidamento anche ai sensi dell'art. 80, comma 5, lettera c-bis del D.lgs. 50/2016, ed eventuale escussione della garanzia provvisoria prestata in favore della Consip, nei casi e nei modi previsti dalla lex specialis di gara;
   b. se la violazione è accertata nella fase successiva all'aggiudicazione ma precedentemente alla stipula dell'Accordo quadro, revoca dell'aggiudicazione ed escussione della garanzia provvisoria;
   c. se la violazione è accertata nella fase di esecuzione:

      risoluzione *ex* art. 1456 c.c. dell'Accordo Quadro, nonché incameramento della garanzia definitiva e risarcimento dell'eventuale danno ulteriore, nel caso in cui la violazione degli impegni di cui al precedente art. 3 sia accertata in relazione agli obblighi contrattuali assunti dal Fornitore nei confronti di Consip in forza dell'Accordo Quadro. La risoluzione può essere altresì esercitata ai sensi dell'art. 1456 c.c. i) ogni qualvolta nei confronti del Fornitore, dei suoi dirigenti e/o dei componenti della compagine sociale, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319bis, 319ter, 319quater, 320, 322, 322bis, 346bis, 353, 353bis, 355 e 356 c.p. ii) nel caso in cui, violato l'obbligo di segnalazione di cui all'art. 3, lett. e2) che precede, sia stata disposta nei confronti dei "pubblici amministratori"[1] che hanno esercitato funzioni relative alla stipula ed esecuzione del contratto, misura cautelare o sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 del c.p.. Nei casi sopra indicati sub i) e ii), Consip eserciterà la potestà risolutoria previa intesa con l'Autorità Nazionale Anticorruzione che potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto Contrattuale alle condizioni di cui all'art. 32 del D.L. 90/2014 convertito nella legge n. 114/2014. Resta fermo che dell'intervenuta risoluzione dell'Accordo Quadro Consip potrà tenere conto ai fini delle valutazioni di cui all'articolo 80, comma 5, lett. c-ter), del D.Lgs. 50/2016.

      La risoluzione dell'Accordo Quadro prevista nel presente Patto di Integrità può costituire condizione risolutiva del singolo Contratto esecutivo;

      risoluzione *ex* art. 1456 c.c. del singolo Contratto esecutivo, nel caso in cui la violazione degli impegni di cui al precedente art. 3 sia accertata in relazione agli obblighi contrattuali assunti dal Fornitore nei confronti della singola Amministrazione contraente nell'ambito del Contratto esecutivo. La risoluzione potrà essere altresì esercitata ai sensi dell'art. 1456 c.c. i) ogni qualvolta nei confronti del Fornitore, dei suoi dirigenti e/o dei componenti della compagine sociale, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319bis, 319ter, 319quater, 320, 322, 322bis, 346bis, 353, 353bis, 355 e 356 c.p.; ii) nel caso in cui, violato l'obbligo di segnalazione di cui all'art. 3, lett. e2) che precede, sia stata disposta nei confronti dei "pubblici amministratori" che hanno esercitato funzioni relative alla stipula ed esecuzione del contratto, misura cautelare o sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 del c.p.. Nei casi sopra indicati sub i) e ii) l'Amministrazione eserciterà la potestà risolutoria previa intesa con l'Autorità Nazionale Anticorruzione che potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto contrattuale alle condizioni

[1] Per "pubblici amministratori" si intendono i soggetti che hanno esercitato attività di pubblico interesse.

di all'art. 32 del D.L. 90/2014 convertito nella legge n. 114/2014.

La risoluzione del singolo Contratto esecutivo comporterà altresì l'escussione della garanzia definitiva.

In caso di intervenuta risoluzione del Contratto esecutivo su iniziativa della singola Amministrazione contraente, quest'ultima è tenuta a darne tempestiva notizia a Consip, motivandone le ragioni; Consip, a sua volta, ha la facoltà di procedere, ai sensi dell'art. 1456 c.c., alla risoluzione di diritto dell'Accordo Quadro. Resta fermo che dell'intervenuta risoluzione Contratto esecutivo Consip potrà tenere conto ai fini delle valutazioni di cui all'articolo 80, comma 5, lett. c-ter), del D.Lgs. 50/2016;

In ogni caso Consip procederà alla segnalazione del fatto all'ANAC ed alle competenti Autorità giurisdizionali.

ART. 6 AUTORITÀ COMPETENTE IN CASO DI CONTROVERSIE

Ogni eventuale controversia relativa all'interpretazione e all'esecuzione del presente Patto di Integrità sarà risolta dall'Autorità Giudiziaria competente, secondo quanto nell'Accordo Quadro.

Roma, lì ___ ___

Il presente Patto di integrità viene allegato quale parte integrante dell'Accordo Quadro.

ALLEGATO E – NOMINA E RESPONSABILE DEL TRATTAMENTO DATI

CONTRATTO ESECUTIVO NELL'AMBITO DELL'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

NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI

1. Con la sottoscrizione della presente da parte dell'Amministrazione _____ 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 attuativo (nel seguito anche "contratto") relativo alla Convenzione _____. 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 dell'Amministrazione (Titolare del Trattamento), **le sole operazioni di trattamento necessarie per fornire il servizio oggetto del contratto attuativo e della Convenzione**, nei limiti delle finalità ivi specificate, nel rispetto del Regolamento UE 2016/679, del D.Lgs. 196/2003 e s.m.i e del D. Lgs. n. 101/2018 (nel seguito anche *"Normativa in tema di trattamento dei dati personali"*), e delle istruzioni nel seguito fornite.
2. Il Fornitore/Responsabile si impegna a presentare su richiesta dell'Amministrazione 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. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.
3. Le finalità del trattamento sono: ***<Valorizzare in ragione dell'oggetto del contratto _____>***
4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: ***<Valorizzare in ragione dell'oggetto del contratto*** i) dati comuni (es. dati anagrafici e di contatto ecc.); ii) dati sensibili; iii) dati giudiziari***>***.
5. Le categorie di interessati sono: ***<Valorizzare in ragione dell'oggetto del contratto*** es. dipendenti e collaboratori, utenti dei servizi, ecc.>.
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 personali 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 al Responsabile;
   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) 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 dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, 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) ***<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***, ai sensi dell'art. 30 del Regolamento UE e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione 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 >;

i) <***eventuale***: adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla Circolare AgID n. 2/2017 del 18 aprile 2017>.

7. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Fornitore si impegna a fornire all'Amministrazione un piano di misure di sicurezza rimesse all'approvazione della stessa, che saranno concordate al fine di 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.

    La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.
8. 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 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 <***o diverso termine indicato dalla PA*** > giorni lavorativi,; 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, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà le penali previste nella Convenzione e diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

9. ***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 _____ ***(la PA deve specificare la periodicità)***, il Titolare del trattamento delle nomine e delle sostituzioni dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi dei sub-Responsabili nominati 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.
10. 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 chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro 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 o risulti che il sub responsabile agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà al Fornitore/Responsabile Inziale del trattamento le penali previste nella Convenzione e diffiderà lo stesso a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il contratto attuativo con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ***<selezionare una tra le due opzioni:***
1) ad informare tempestivamente il Titolare del trattamento, fornendo adeguato riscontro agli interessati, in nome e per conto del Titolare del trattamento, nei termini previsti dalla Regolamento UE; ***oppure>***
2) 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.
12. 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 <***da valorizzare in alternativa***: sub-Responsabile> del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

13. 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.
14. 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.
15. 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.
16. Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.
17. 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 contratto attuativo, 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.
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.
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.
20. 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.
21. 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 Protezione dei Dati Personali e/o della disciplina sulla protezione dei dati personali contenuta nella Convezione (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o sub-fornitori.

ALLEGATO F – SCHEMA DI CONTRATTO ESECUTIVO – LOTTO 2

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, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, 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 PAC 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)

ALLEGATO G – DISPOSIZIONI PER LA GOVERNANCE

Piano Strategico ICT
Governance delle Gare Strategiche

Disposizioni per la governance

Categorizzazione, Indicatori di digitalizzazione

Sommario

Indice delle tabelle

1. PREMESSA

Il presente documento illustra gli elementi essenziali della governance delle Gare Strategiche del Piano ICT 2019[1] elaborato da AgID e Consip.
Le misure indicate hanno l'obiettivo di abilitare il monitoraggio di coerenza dei Contratti Esecutivi che saranno sottoscritti dalle Amministrazioni a partire dagli Accordi Quadro stipulati da Consip con gli aggiudicatari di ciascuna Gara Strategica.

2. DEFINIZIONI

- **Categorizzazione:** inquadramento o classificazione rispetto al Piano Triennale per l'Informatica nella Pubblica Amministrazione, ed. 2019-2021 e successive
- **Organismi di coordinamento e controllo**: differenziati in Organismi tecnici e Organismo strategico, sono le Strutture deputate alla governance dell'esecuzione dei Contratti derivanti dalle Gare Strategiche.
- **Organismo tecnico di coordinamento e controllo**: struttura organizzativa, nominata per ciascuna Gara, altresì definito **Comitato Tecnico**. È composto da rappresentanti istituzionali – individuati in AgID e Consip, anche integrati con altri soggetti terzi da questi individuati e da rappresentati del Fornitore/dei Fornitori aggiudicatari della specifica procedura di gara (Gara Strategica).
- **Organismo Strategico di coordinamento e controllo**: struttura organizzativa unica, altresì definita **Comitato Strategico**, per la governance di tutte le gare strategiche del Piano ICT 2019, composta da rappresentanti di AgID, Consip e dal Dipartimento per la Trasformazione digitale, individuati dai medesimi soggetti.
- **Gestione del transiente**: attività, progetti e contratti finalizzati al mantenimento del funzionamento *as is* dei sistemi e delle applicazioni dell'Amministrazione.
- **Contratti ad alta rilevanza**: Contratti Esecutivi caratterizzati da elementi di volume, valore, tecnologia, rilevanza nazionale, di particolare interesse ai fini del coordinamento e controllo operato dal Comitato Strategico.
- **Dati di governance**: principi, categorizzazione, indicatori generali e specifici di digitalizzazione.
- **Valore *ex ante***: si intende la misura rilevata per l'indicatore di riferimento prima dell'avvio delle attività contrattualizzate dall'Amministrazione con il Fornitore e finalizzate al raggiungimento dell'obiettivo del Contratto Esecutivo.
- **Valore *ex post***: si intende la misura rilevata per l'indicatore di riferimento a valle del completamento delle attività contrattualizzate dall'Amministrazione con il Fornitore e finalizzate al raggiungimento dell'obiettivo del Contratto Esecutivo.
- **Intervento:** insieme di più attività svolte mediante i servizi di un contratto Esecutivo; l'intervento è identificato da un obiettivo che l'Amministrazione intende raggiungere con lo svolgimento delle attività che lo compongono.

[1] Comprensivo delle sue evoluzioni.

3. PERIMETRO

Le misure e le modalità descritte nel presente documento si applicano alle seguenti Gare Strategiche:

- Digital Transformation (ID 2069),
- Public Cloud IaaS e PaaS (ID 2213),
- Servizi Applicativi in ottica cloud (ID 2212),
- Data Management (ID 2102),
- Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367),
- Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174),
- Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)[2],
- Sanità digitale 1 - sistemi informativi clinico assistenziali (ID 2202),
- Sanità digitale 2 - sistemi informativi sanitari e servizi al cittadino (ID 2365),
- Sanità digitale 3 - sistemi informativi gestionali (ID 2366),
- Public Cloud SaaS[3].

[2] ID 2296 è bandita ai sensi dell'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, che ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, 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". Per la merceologia trattata è considerata al pari delle gare strategiche.

[3] Tutte le gare che saranno definite.

4. MONITORAGGIO DELL'APPLICAZIONE DEL PIANO TRIENNALE

Al fine di monitorare il recepimento dei principi e delle indicazioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione (più avanti anche solo Piano Triennale), in particolare rispetto alla sua edizione 2020-2022, si aggiorna come di seguito descritto la categorizzazione dei contratti esecutivi che saranno stipulati sugli Accordi Quadro relativi alle Gare Strategiche.

- Riferimento alla documentazione di gara: CT generale delle 4 gare strategiche pubblicate 2019-2020 – Categorizzazione
- Applicabilità: ciascun contratto esecutivo, sia esso derivante da ordine diretto o da rilancio competitivo, non si applica ai contrati esecutivi riferiti alla *gestione del transiente*[4]
- Soggetto impattato: l'Amministrazione che stipula un contratto esecutivo
- Modalità di censimento dell'informazione:
    a) Per i contratti scaturenti da ordine diretto, nel caso di gare che prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate nel Piano dei Fabbisogni e/o nei suoi allegati, in ogni caso secondo standard e modalità messi a disposizione da Consip S.p.A. alla stipula dell'AQ;
    b) Per i contratti scaturenti da ordine diretto, nel caso di gare che non prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate in allegati alla documentazione contrattuale predisposti secondo standard messi a disposizione da Consip S.p.A. alla stipula dell'AQ;
    c) Per i contratti scaturenti da rilancio competitivo, le informazioni dovranno essere esplicitate in allegati alla documentazione contrattuale predisposti secondo standard messi a disposizione da Consip S.p.A., alla stipula dell'AQ;
- Vincoli temporali per la raccolta delle informazioni: in quanto informazioni allegate alla documentazione contrattuale, entro la stipula del contratto esecutivo in caso di ordine diretto, e in allegato alla documentazione di Appalto Specifico in caso di rilancio competitivo.
- Regole di applicazione/calcolo: negli standard forniti da Consip, in via propedeutica rispetto all'esplicitazione della categorizzazione, dei principi e degli indicatori, l'Amministrazione dovrà indicare se il Contratto Esecutivo è riferito alla *gestione del transiente.*

4.1 ELEMENTI CARATTERIZZANTI

Il monitoraggio riguarda:

- i **principi guida** che l'Amministrazione prevede di seguire attraverso la realizzazione delle attività oggetto l'ordine/AS;
- la **categorizzazione**, cioè la mappatura, del Contratto Esecutivo, stipulato dall'Amministrazione, rispetto agli ambiti (layer) del Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022.

[4] Come definita nel par. 2 - Definizioni

5. PRINCIPI GUIDA

L'Amministrazione, in maniera facoltativa, potrà indicare i principi guida che prevede di seguire attraverso l'ordine/AS, selezionando uno o più dei seguenti, in base alla applicabilità allo specifico AQ di riferimento:

- *Digital & mobile first* (digitale e mobile come prima opzione): le Pubbliche Amministrazioni devono realizzare servizi primariamente digitali;
- *digital identity only* (accesso esclusivo mediante identità digitale): le Pubbliche Amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;
- *cloud first* (cloud come prima opzione): le Pubbliche Amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;
- servizi inclusivi e accessibili: le Pubbliche Amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- dati pubblici un bene comune: il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- interoperabile by design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- sicurezza e *privacy by design*: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- *user-centric*, *data driven* e *agile*: le Amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.
- *once only*: le Pubbliche Amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;
- transfrontaliero *by design* (concepito come transfrontaliero): le Pubbliche Amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- *open source*: le Pubbliche Amministrazioni devono prediligere l'utilizzo di software con codice sorgente aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

6. CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI RISPETTO AL PIANO TRIENNALE 2020-2022

Per ciascun Contratto Esecutivo, ad esclusione di quanto soggetto a segreto di Stato e delle classifiche di segretezza, l'Amministrazione avrà l'**obbligo**[5] di indicare gli ambiti (o *layer*) – cosiddetti di I livello - e i relativi obiettivi del Piano Triennale che essa prevede di mappare mediante le attività che saranno svolte con il Contratto esecutivo in oggetto.
Per ciascuno degli ambiti scelti, l'Amministrazione potrà selezionare, tra quelli presenti, uno o più obiettivi.
La categorizzazione prevede:

- un inquadramento di I livello, che si applica a tutti i contratti esecutivi;
- un inquadramento di II livello, che si applica solo ai contratti esecutivi definiti ad "alta rilevanza" secondo i criteri più appresso definiti per ciascuna Gara Strategica.

6.1 CATEGORIZZAZIONE DI I LIVELLO DEI CONTRATTI ESECUTIVI

La seguente tabella sintetizza la Categorizzazione e gli obiettivi associati:

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

[5] Come da CT generale delle Gare strategiche pubblicate 2019-2020.

Ambito I livello (layer)	Obiettivi Piano Triennale
Infrastrutture	• 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
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

Tabella 1 - Obiettivi del Piano Triennale

Rispetto alla categorizzazione completa di cui alla Tabella 1 - Obiettivi del Piano Triennale, per ciascuna Gara Strategica si individuano nei seguenti paragrafi i layer applicabili.

6.1.1 CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE PUBBLICATE 2019-2020

Gara Strategica	Ambito I livello applicabile
Digital Transformation	• Servizi • Dati • Piattaforme • Infrastrutture • Interoperabilità • Sicurezza Informatica
Public Cloud IaaS e PaaS	• Servizi • Infrastrutture • Dati
Servizi applicativi in ottica cloud	• Servizi • Piattaforme • Interoperabilità
Data Management	• Dati

Tabella 2 - Categorizzazione di I livello (Gare Strategiche pubblicate 2019-2020)

6.1.2 CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE IN PREDISPOSIZIONE

Per le seguenti iniziative:

- Fornitura di prodotti per la sicurezza perimetrale, protezione degli end point e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367),
- Fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174),
- Fornitura di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – (ID 2296),

Si applicano almeno gli ambiti di I livello *Sicurezza Informatica* e *Infrastrutture.*

- Per le Gare Strategiche SaaS varrà tutto quanto specificato per il solo Lotto 1 della Public Cloud.
- Per le Gare Strategiche di Sanità Digitale, la categorizzazione sarà definita in documentazione di gara, compatibilmente con i tempi già previsti per la pubblicazione dei bandi, o comunque nel corso delle attività propedeutiche alla stipula dei relativi AQ.

6.2 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI

Per i contratti ad *alta rilevanza* le Amministrazioni contraenti dettagliano i dati forniti secondo quanto indicato nel seguito.
Le informazioni relative alla categorizzazione sono fornite con le stesse modalità e tempistiche previste per la categorizzazione di I livello (cfr. par. 6.1)
In particolare, le Amministrazioni provvedono a:

1. Raffinare le indicazioni sugli ambiti di I livello (layer), indicando gli ambiti di II livello mediante una selezione, anche multipla, dalla categorizzazione riportata nella seguente tabella:

Ambito I (layer)	Ambito II livello
Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
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
Piattaforme	• Sanità digitale (FSE e CUP) • Identità Digitale; • Pagamenti digitali; • App IO; • ANPR; • NoiPA; • INAD; • Musei; • Siope+
Infrastrutture	• Data Center e Cloud • Connettività
Interoperabilità	• Agricoltura, pesca, silvicoltura e prodotti alimentari • Economia e finanze • Istruzione, cultura e sport • Energia • Ambiente

Ambito I (layer)	Ambito II livello
	• Governo e Settore pubblico • Salute • Tematiche internazionali • Giustizia e sicurezza pubblica • Regioni e città • Popolazione e società • Scienza e tecnologia • Trasporti
Sicurezza informatica	• Portali istituzionali e CMS • Sensibilizzazione del rischio cyber

Tabella 3 - Categorizzazione generale di II livello

6.2.1 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE PUBBLICATE 2019-2020

Nell'applicazione di quanto sopra descritto, l'amministrazione terrà conto degli ambiti applicabili come già descritti per la categorizzazione di I livello e riportati nella seguente tabella:

Gara strategica	Ambito I livello applicabile	Ambito II livello applicabile
Digital Transformation	Tutti	Tutti
Public Cloud IaaS e PaaS	• Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
	• Infrastrutture	• 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
	• Dati	• Data Center e Cloud • Connettività
Servizi applicativi in ottica cloud	• 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+
	• Interoperabilità	• 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
Data Management	• 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

Tabella 4 - Categorizzazione di II livello (Gare Strategiche pubblicate 2019-2020)

6.2.2 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE IN PREDISPOSIZIONE

Fermo restando l'obbligo per le Amministrazioni di indicare gli ambiti di I livello e i relativi obiettivi del Piano Triennale, per le iniziative di Sicurezza Informatica ci si riserva la possibilità di definire prima della stipula dell'Accordo Quadro eventuali ambiti di II Livello più specifici per una mappatura più mirata degli interventi in ambito Cyber Security da parte delle PA.

Per le altre iniziative la categorizzazione di II livello sarà definita congiuntamente ad AgID e al Dipartimento in tempo utile per la stipula dei relativi contratti di AQ.

6.3 CONTRATTI AD ALTA RILEVANZA

Nel seguente paragrafo si riportano, per ciascuna delle Gare Strategiche pubblicate nel periodo 2019-2020 (Digital Transformation, Public Cloud IaaS e PaaS, Servizi applicativi in ottica cloud e Data Management), le caratteristiche di rilevanza individuate in funzione delle peculiarità dei servizi e degli obiettivi della gara di riferimento.
Si precisa che, in ogni caso, il Comitato Strategico potrà includere nel novero dei contratti ad alta rilevanza anche altre tipologie, quali ad esempio i contratti inerenti l'interoperabilità, le piattaforme abilitanti e in generale, rilevanti ai fini del processo di avanzamento della trasformazione digitale e dell'adozione del modello Cloud nella PA.
Per le Gare strategiche in predisposizione:

- Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367);
- Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174);
- Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296);

e per le Gare Strategiche attinenti alla Sanità digitale, ci si riserva la possibilità di definire prima della stipula degli Accordi Quadro i criteri per l'identificazione dei Contratti Esecutivi *ad alta rilevanza.*

Gara strategica	Lotto	criteri	indicatori aggiuntivi
Digital Transformation	Lotto 1 Lotto 2	• Lotto 1: Contratti Esecutivi di importo > € 450.000,00 i.e. • Lotto 2: Contratti Esecutivi di importo > € 400.000,00 i.e.	• Non si prevedono indicatori aggiuntivi per i contratti esecutivi ad alta rilevanza. • Per i Lotti dal 3 al 9, trattandosi di lotti di servizi complementari a quelli previsti per Lotto 1 e Lotto 2, non si prevedono soglie specifiche.
Public Cloud IaaS e PaaS		• Lotto 1: Contratti Esecutivi che includono più di 3 categorie di servizi del configuratore; oppure Contratti Esecutivi di importo > € 500.000,00 i.e. • Lotti 2-11: contratti esecutivi > € 250.000,00 i.e.	Nessun indicatore aggiuntivo

Gara strategica	Lotto	criteri	indicatori aggiuntivi
Servizi applicativi in ottica *cloud*		• Lotti 1 e 2: Contratti Esecutivi di importo > € 10.000.000,00 i.e. • Lotti 3,4,5: n.a. • Lotti 6,7,8,9: n.a.	Previsti (cfr. 7.3.3)
Data Management		• Lotti 1,2,3: Contratti Esecutivi di importo > € 1.000.000,00 i.e.	Previsti (cfr 7.3.4)

Tabella 5 - Criteri per l'identificazione dei Contratti Esecutivi ad *alta rilevanza*

Per quanto riguarda le Gare Strategiche in predisposizione, eventuali criteri per identificare Contratti ad alta rilevanza saranno definiti entro la stipula, congiuntamente ad AgID e Dipartimento.

7. MONITORAGGIO DEI RISULTATI DI DIGITALIZZAZIONE

Al fine di abilitare un puntuale monitoraggio dei risultati ottenuti dalle Amministrazioni in termini di digitalizzazione mediante l'utilizzo degli Accordi Quadro relativi alle Gare Strategiche sono stati previsti, in documentazione di gara, ed articolati nel presente documento indicatori così classificati:

- **Indicatori Generali di digitalizzazione**, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale;
- **Indicatori Specifici di digitalizzazione**, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti.

Gli indicatori sono utilizzati per il monitoraggio dei contratti e del raggiungimento dei relativi obiettivi, così come dettagliati nel Piano dei Fabbisogni e nel Piano Operativo.
Ciascuna Amministrazione, all'atto di definizione del Piano dei Fabbisogni o altra specifica documentazione contrattuale laddove il Piano dei Fabbisogni non sia previsto, individuerà almeno un Indicatore Generale per il quale fornirà, agli Organismi di coordinamento e controllo e/o ai soggetti da questi indicati, le misure di riferimento ex ante ed ex post rispetto al contratto esecutivo.

7.1 INDICATORI GENERALI DI DIGITALIZZAZIONE

- Riferimento alla documentazione di gara: CT generale delle 4 gare strategiche pubblicate 2019-2020 – Categorizzazione
- Applicabilità: ciascun contratto esecutivo, sia esso derivante da ordine diretto o da rilancio competitivo, ad esclusione di quelli relativi alla *gestione del transiente o che includono unicamente servizi di gestione e/o di supporto,* ad esclusione di quanto soggetto a segreto di Stato e delle classifiche di segretezza
- Soggetto impattato: l'Amministrazione che stipula un contratto esecutivo
- Modalità di raccolta dell'informazione:
    a) Per i contratti scaturenti da ordine diretto, nel caso di gare che prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate nel Piano dei Fabbisogni e/o nei suoi allegati;
    b) Per i contratti scaturenti da ordine diretto, nel caso di gare che non prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate in allegati alla documentazione contrattuale predisposti secondo standard messi a disposizione da Consip S.p.A. alla stipula dell'AQ;
    c) Per i contratti scaturenti da rilancio competitivo, le informazioni dovranno essere esplicitate in allegati alla documentazione di gara relativa all'AS, predisposti secondo standard messi a disposizione da Consip S.p.A.
- Vincoli temporali per la scelta degli indicatori: in quanto informazioni allegate alla documentazione contrattuale, entro la stipula del contratto esecutivo in caso di ordine diretto, e contestualmente alla pubblicazione dell'Appalto Specifico, in allegato alla documentazione in caso di rilancio competitivo; in alternativa, per le gare in ambito Sicurezza, in caso di ordine diretto senza Piano dei Fabbisogni, entro la data di emissione del Piano di Lavoro Generale.

La misura *ex post* sarà fornita, al completamento delle attività contrattuali, con un aggiornamento degli allegati utilizzati per fornire i dati di governance, con particolare riferimento agli indicatori di digitalizzazione, e tracciato nel portale del Fornitore che ha eseguito l'intervento oggetto di misura, nei tempi previsti per l'aggiornamento dei dati sul Portale stesso.

- Regole di applicazione/calcolo: in via propedeutica rispetto all'esplicitazione della categorizzazione, dei principi e degli indicatori, l'Amministrazione dovrà indicare, negli standard forniti da Consip, se il Contratto Esecutivo è riferito alla *gestione del transiente.*

Gli indicatori generali di digitalizzazione, validi per tutte le Gare Strategiche, sono i seguenti:

Indicatori quantitativi	Indicatori qualitativi	Indicatori di collaborazione e riuso
Riduzione % della spesa per l'erogazione del servizio	Obiettivi CAD raggiunti con l'intervento	Riuso di processi per erogazione servizi
Riduzione % dei tempi di erogazione del servizio	Integrazione con infrastrutture immateriali	Riuso soluzioni tecniche
Numero servizi aggiuntivi offerti all'utenza interna, esterna (cittadini), esterna (imprese), altre PA	Integrazione con Basi Dati di interesse nazionale	Collaborazione con altre Amministrazioni (progetto in co-working, realizzato anche mediante contratti esecutivi diversi per Amministrazione)

Tabella 6 - Indicatori Generali di digitalizzazione

Per le gare di Sicurezza[6] non è prevista la scelta degli indicatori sopra riportati: i servizi erogati dalle gare infatti, non consentono di costruire logicamente una correlazione tra il servizio acquistato dall'Amministrazione e il contenuto degli indicatori generali.
Nelle seguenti tabelle si riportano le modalità di misurazione degli indicatori generali.

Si precisa che per tutti gli indicatori generali di digitalizzazione:

1. L'oggetto di riferimento è sempre il Contratto Esecutivo;
2. Nel caso in cui con uno stesso Contratto Esecutivo l'Amministrazione voglia realizzare uno o più interventi progettuali, potrà
   - Scegliere l'indicatore con riferimento all'intervento più rilevante in termini di effort/spesa per la realizzazione dello stesso,

[6] *Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni* (ID 2367); *Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni* (ID 2174); *Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni* (ID 2296)

- Scegliere più indicatori riferendone ciascuno ad uno degli interventi la cui realizzazione è prevista con l'acquisizione dei servizi del Contratto Esecutivo.

L'Amministrazione dovrà quindi specificare, secondo gli standard messi a disposizione da Consip, le informazioni relative alla scelta sopra formulata e successivamente, in fase di raccolta del *valore ex post*, specificare, nel caso di più interventi, a quale intervento il valore si riferisce.

Indicatori quantitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Riduzione % della spesa per l'erogazione del servizio	IQT1	Il riferimento è al **servizio digitale erogato dall'Amministrazione** verso la sua utenza. L'indicatore misura la variazione della spesa, sostenuta dall'Amministrazione e intesa come **costo stimato per l'erogazione del servizio digitale, per unità di servizio digitale erogato all'utenza.** La variazione è espressa in % e prende in considerazione: • Il costo attuale sostenuto dall'Amministrazione per l'erogazione di una unità di servizio digitale, calcolato prima dell'avvio delle attività del Contratto Esecutivo di pertinenza[7] • Il costo aggiornato sostenuto dall'Amministrazione per l'erogazione di una unità di servizio digitale, calcolato a valle del completamento delle attività del Contratto Esecutivo di pertinenza. Nello stimare il costo l'Amministrazione terrà conto delle componenti hw, sw, di risorse professionali per la gestione interna e idealmente il TCO, qualora disponibile.	• Valore *ex ante* rispetto all'intervento[8], in termini di **stima della riduzione del costo per l'erogazione del servizio digitale, per unità di servizio digitale erogato**; • Valore *ex post*, al completamento dell'intervento[9], in termini di **misura effettiva della riduzione del costo per l'erogazione del servizio digitale, per unità di servizio digitale erogato**

[7] Nel caso in cui le attività riguardino uno o più interventi inclusi nel Contratto Esecutivo, l'Amministrazione terrà conto solo di quelli pertinenti al raggiungimento dell'obiettivo e quindi coerenti con l'indicatore scelto.
[8] o agli interventi di pertinenza come esplicitato nelle modalità di misura.
[9] Vedi nota precedente.

Indicatori quantitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Riduzione % dei tempi di erogazione del servizio	IQT2	Il riferimento è al **servizio digitale erogato dall'Amministrazione** verso la sua utenza. L'indicatore misura la variazione del tempo di erogazione del servizio digitale da parte dell'Amministrazione e inteso come **il tempo intercorrente tra la "richiesta", da parte dell'utente del servizio digitale verso l'Amministrazione, e la disponibilità dell'oggetto del servizio** all'utente stesso. La variazione è espressa in % e prende in considerazione: • Il tempo attuale intercorrente tra la richiesta da parte dell'utente dell'Amministrazione mediante il servizio digitale, per l'erogazione di una unità di servizio digitale, calcolato prima dell'avvio delle attività del Contratto Esecutivo di pertinenza[10] • Il tempo aggiornato intercorrente tra la richiesta da parte dell'utente dell'Amministrazione mediante il servizio digitale, per l'erogazione di una unità di servizio digitale, calcolato a valle del completamento delle attività del Contratto Esecutivo di pertinenza[11]	• Valore *ex ante* rispetto all'intervento[12], in termini di **stima della riduzione del tempo di erogazione del servizio digitale, per unità di servizio digitale erogato**; • Valore *ex post*, al completamento dell'intervento[13], in termini di **misura effettiva della riduzione del tempo di erogazione del servizio digitale, per unità di servizio digitale erogato.**

[10] Nel caso in cui le attività riguardino uno o più interventi inclusi nel Contratto Esecutivo, l'Amministrazione terrà conto solo di quelli pertinenti al raggiungimento dell'obiettivo e quindi coerenti con l'indicatore scelto.
[11] Vedi nota precedente.
[12] o agli interventi di pertinenza come esplicitato nelle modalità di misura.
[13] Vedi nota precedente.

Indicatori quantitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Numero servizi aggiuntivi offerti all'utenza interna, esterna (cittadini), esterna (imprese), altre PA	IQT3	Quantità di **nuovi servizi digitali che l'Amministrazione mette a disposizione della propria utenza**, utilizzando le risorse messe a disposizione dal Contratto Esecutivo; La quantità è espressa in termini assoluti, per ciascuna tipologia di utente.	• Valore *ex ante* rispetto all'intervento[14], in termini di **numero di nuovi servizi digitali che l'Amministrazione intende realizzare e mettere a disposizione della propria utenza mediante il Contratto Esecutivo**; • Valore **ex post**, al completamento dell'intervento[15], in termini di numero effettivo di nuovi servizi digitali **che l'Amministrazione ha messo a disposizione della propria utenza mediante il Contratto Esecutivo.**

Tabella 7 - Indicatori Generali quantitativi

[14] o agli interventi di pertinenza come esplicitato nelle modalità di misura.
[15] Vedi nota precedente.

Indicatori qualitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Obiettivi CAD raggiunti con l'intervento[16]	IQL1	Selezione ed indicazione[17]di uno o più obiettivi CAD[18]: • Diritto all'uso delle tecnologie • Partecipazione al procedimento amministrativo informatico • Effettuazione dei pagamenti con modalità informatiche • Utilizzo della posta elettronica certificata • Qualità dei servizi resi e soddisfazione dell'utenza • Alfabetizzazione informatica dei cittadini • Partecipazione democratica elettronica • Sportelli per le attività produttive • Registro informatico degli adempimenti amministrativi per le imprese	• Valore *ex ante* rispetto all'intervento[19], in termini di **indicazione degli obiettivi CAD che l'amministrazione intende raggiungere con le attività previste in Contratto Esecutivo;** • Valore *ex post* rispetto all'intervento[20], in termini di **indicazione degli obiettivi CAD effettivamente raggiunti dall'Amministrazione con le attività previste in Contratto Esecutivo.**

[16] Anche in questo caso, l'Amministrazione può far riferimento alle attività previste dall'intero contratto esecutivo, oppure ad una sua parte (uno o più interventi).
[17] Mediante gli strumenti e/o gli standard messi a disposizione da Consip.
[18] Gli obiettivi sono quelli riportati nella "**Sezione II. Diritti dei cittadini e delle imprese" del "Capo I Principi generali** del CAD. La selezione sarà fatta sullo standard fornito da Consip.
[19] o agli interventi di pertinenza come esplicitato nelle modalità di misura.
[20] o agli interventi di pertinenza come esplicitato nelle modalità di misura.

Indicatori qualitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Integrazione con infrastrutture immateriali	IQL2	Selezione ed indicazione[21]di una o più infrastrutture immateriali di cui al Piano Triennale.	• Valore *ex ante* rispetto all'intervento[22], in termini di **indicazione delle infrastrutture immateriali che l'Amministrazione intende integrare con le attività previste in Contratto Esecutivo;** • Valore *ex post* rispetto all'intervento[23], in termini di **indicazione delle infrastrutture effettivamente integrate dall'Amministrazione con le attività previste in Contratto Esecutivo.**

[21] Mediante gli strumenti e/o gli standard messi a disposizione da Consip.
[22] o agli interventi di pertinenza come esplicitato nelle modalità di misura.
[23] o agli interventi di pertinenza come esplicitato nelle modalità di misura.

Indicatori qualitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Integrazione con Basi Dati di interesse nazionale	IQL3	Selezione ed indicazione[24]di una o più Basi Dati di interesse nazionale.	• Valore *ex ante* rispetto all'intervento[25], in termini di **indicazione delle Basi Dati di interesse nazionale che l'Amministrazione intende integrare con le attività previste in Contratto Esecutivo;** • Valore *ex post* rispetto all'intervento[26], in termini di **indicazione delle Basi Dati di interesse nazionale effettivamente integrate dall'Amministrazione con le attività previste in Contratto Esecutivo.**

Tabella 8 - Indicatori Generali qualitativi

[24] Mediante gli strumenti e/o gli standard messi a disposizione da Consip.
[25] o agli interventi di pertinenza come esplicitato nelle modalità di misura.
[26] o agli interventi di pertinenza come esplicitato nelle modalità di misura.

Indicatori di collaborazione e riuso	ID	Modalità di misura	Rilevazione dell'indicatore
Riuso di processi per erogazione servizi	ICR1	Indicazione dei processi (e laddove applicabile), del loro numero e delle Amministrazioni delle quali si riutilizza il processo	• Valore *ex ante*: **elencazione dei processi** e delle Amministrazioni di riferimento del riuso dei processi **che l'Amministrazione intende riusare** nel Contratto Esecutivo; • Valore *ex post*: elencazione dei **processi effettivamente riusati dall'Amministrazione** nelle attività del Contratto Esecutivo.
Riuso soluzioni tecniche	ICR2	Indicazione delle soluzioni tecniche riutilizzate e della/delle Amministrazione/i della/e quale/i si riutilizzano le soluzioni	• Valore *ex ante*: **elencazione delle soluzioni tecniche** e delle Amministrazioni di riferimento **che l'Amministrazione intende riusare** nel Contratto Esecutivo; • Valore *ex post*: elencazione **delle soluzioni tecniche effettivamente riusate dall'Amministrazione** nelle attività del Contratto Esecutivo.

Indicatori di collaborazione e riuso	ID	Modalità di misura	Rilevazione dell'indicatore
Collaborazione con altre Amministrazioni (progetto in co-working)	ICR3	Indicazione delle Amministrazioni coinvolte nel progetto[27] in coworking	• Valore *ex ante*: **elencazione delle Amministrazioni coinvolte nella realizzazione del progetto in coworking con le quali l'Amministrazione collaborerà utilizzando le risorse del** Contratto Esecutivo; • Valore *ex ante*: **elencazione delle Amministrazioni con le quali l'Amministrazione ha effettivamente collaborato.**

Tabella 9 - Indicatori generali di riuso

Eventuali ulteriori elementi di dettaglio per la rilevazione degli indicatori generali saranno forniti alla stipula/attivazione dell'Accordo Quadro, o comunque secondo le modalità e i tempi concordati dall'Organismo di Coordinamento e Controllo finalizzato alla direzione strategica e/o secondo quanto più precisamente definito in corso d'opera all'atto della stipula/attivazione degli Accordi Quadro delle Gare Strategiche Digital Transformation, Public Cloud IaaS e PaaS, Servizi Applicativi in ottica cloud e Data Management.

Si precisa che, fatte salve le previsioni della documentazione di gara

- I valori *ex ante* dovranno essere forniti secondo gli standard messi a disposizione da Consip e comunque allegati alla documentazione contrattuale del Contratto Esecutivo, nel caso di Ordini, e allegati alla documentazione di AS nel caso di rilancio competitivo;
- I valori *ex post* dovranno essere forniti dall'Amministrazione, con il supporto del Fornitore, entro la chiusura formale del Contratto Esecutivo e resi disponibili sul Portale del Fornitore nei tempi previsti per l'aggiornamento periodico.

[27] Per progetto si intende in questo caso un insieme complesso di attività realizzato in coworking da più Amministrazioni, ciascuna mediante uno o più contratti esecutivi volti a realizzare uno o più interventi funzionali alla realizzazione del progetto in coworking.

7.2 INDICATORI SPECIFICI DI DIGITALIZZAZIONE

Sono individuati sulla base delle caratteristiche specifiche dei servizi, individuati nella documentazione di gara o – laddove previsto – demandati alle valutazioni degli Organismi di coordinamento e controllo. Laddove non presenti in documentazione di gara, le modalità di rilevazione e le relative tempistiche saranno oggetto di specifiche appendici contrattuali per ciascuna gara.

7.2.1 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA DIGITAL TRANSFORMATION

Lotto/servizio	ID	Indicatori specifici
L1.S1 Disegno strategia digitale	DTL1S1.1	• disponibilità piano economico-finanziario (collegato all'implementazione della strategia)
	DTL1S1.2	• numero di linee del Piano Triennale indirizzate nella strategia rispetto al totale delle linee applicabili
	DTL1S1.2	• numero di obiettivi pianificati a 3 anni sul totale obiettivi pianificati nella strategia
L1.S2 Disegno del Piano Strategico ICT	DTL1S2.1	• disponibilità piano economico-finanziario (collegato all'implementazione del Piano Strategico ICT)
	DTL1S2.2	• numero di linee del Piano Triennale indirizzate nella strategia rispetto al totale delle linee applicabili
	DTL1S2.3	• numero di obiettivi pianificati a 3 anni sul totale obiettivi pianificati nella strategia
	DTL1S2.4	• efficientamento atteso della spesa ICT
L1.S3 [28] Disegno della mappa dei servizi digitali dell'Amministrazione	DTL1S3.1	• % servizi digitali mappati rispetto al totale servizi digitali erogati dall'Amministrazione
	DTL1S3.2	• Numero di nuovi servizi digitali mappati rispetto al totale dei servizi digitali erogati dall'Amministrazione
L2.S1	DTL2S1.1	• % servizi digitali con modello di erogazione disegnato/censito rispetto al totale servizi digitali erogati dall'Amministrazione

[28] In valutazione la fattibilità di inserimento di un indicatore volto a misurare il totale dei servizi erogati dall'Amministrazione

Lotto/servizio	ID	Indicatori specifici
Disegno del modello di erogazione del servizio digitale	DTL2S1.2	• % servizi digitali con nuovo modello di erogazione rispetto al totale servizi digitali erogati dall'Amministrazione
L2.S2 Disegno del processo digitale sotteso all'erogazione del servizio digitale	DTL2S2.1	• numero di processi digitali sottesi all'erogazione di servizi disegnati ex novo
	DTL2S2.2	• numero di processi digitali reingegnerizzati
	DTL2S2.3	• numero di servizi digitalizzati end to end per ogni milestone di pianificazione
L2.S3 Supporto specialistico per le attività propedeutiche all'implementazione del servizio digitale	DTL2S3.1	<u>per Supporto alla definizione di interventi di riorganizzazione e Supporto al disegno del processo sotteso al servizio digitale:</u> • Rapporto tra valore (spesa) per supporto e valore dell'intervento di disegno dei processi digitali per il quale si richiede supporto
	DTL2S3.2	<u>per Supporto alla definizione di interventi di riorganizzazione e Supporto al disegno del processo sotteso al servizio digitale:</u> • Rapporto tra numero di processi digitali e numero di giornate di supporto acquistate
	DTL2S3.3	<u>per Supporto alla valutazione degli strumenti di acquisizione</u> • Rapporto tra valore (spesa) per supporto e valore dell'intervento di trasformazione per il quale l'Amministrazione richiede supporto
	DTL2S3.4	<u>per Supporto alla valutazione degli strumenti di acquisizione</u> • Rapporto tra Numero di strumenti di acquisizione valutati mediante l'attività di supporto e numero di giornate di supporto acquistate
L3.S1, L4.S1, L5.S1 Progettazione della Transizione Digitale	-	Non previsti
L3.S2, L4.S2, L5.S2 Affiancamento alla Transizione Digitale	DTL3S2.1 DTL4S2.1 DTL5S2.1	• % di utenti formati sul totale utenti previsti
	DTL3S2.2 DTL4S2.2 DTL5S2.2	• livello di adozione del contenuto di trasformazione digitale.

Lotto/servizio	ID	Indicatori specifici
L6.S1, L7.S1, L8.S1 PMO di programmi di digitalizzazione	-	Non previsti
L6.S2, L7.S2, L8.S2 PMO di progetti cross ambito	-	Non previsti
L6.S3, L7.S3, L8.S3 Supporto alla gestione dei progetti e dei programmi collegati alla Digital Transformation	-	Non previsti
L9.S1 Supporto alla Governance	-	Non previsti

Tabella 10 - Indicatori Specifici Digital Transformation

7.2.2 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA PUBLIC CLOUD IAAS E PAAS

Lotto/Servizio	ID	Indicatori
LOTTO 1 SERVIZI IAAS: • Categoria Compute; • Categoria Storage; • Categoria Network; • Categoria Security; • Categoria Monitoring.	PCL1I.1	• Layer INFRASTRUTTURE: ✓ Riduzione % di RAM disponibile su data center
	PCL1I.2	• Layer INFRASTRUTTURE: ✓ Riduzione % di CPU disponibile su data center
	PCL1I.3	• Layer INFRASTRUTTURE: ✓ Riduzione % di Storage disponibile su data center
	PCL1I.4	• Layer SERVIZI: ✓ Numero di servizi cloud qualificati acquistati
LOTTO 1 SERVIZI PAAS: ○ Categoria Containers; ○ Categoria Database; ○ Categoria Developer Tools; ○ Categoria Application Platform.	PCL1P.1	• Layer INFRASTRUTTURE: ✓ Riduzione % di RAM disponibile su data center
	PCL1P.2	• Layer INFRASTRUTTURE: ✓ Riduzione % di CPU disponibile su data center
	PCL1P.3	• Layer INFRASTRUTTURE: ✓ Riduzione % di Storage disponibile su data center
	PCL1P.4	• Layer SERVIZI: ✓ Numero di servizi cloud qualificati acquistati
LOTTI 2-6 • ASSESSMENT (S1) • STRATEGIA DI MIGRAZIONE (S2) • CHECK DEI RISULTATI (S5)	PCL2.1 PCL3.1 PCL4.1 PCL5.1 PCL6.1	• Layer SERVIZI: ✓ Numero di servizi digitali esistenti erogati in modalità on-premise oggetto di assessment
	PCL2.2 PCL3.2 PCL4.2 PCL5.2 PCL6.2	• Layer SERVIZI: ✓ Numero di servizi migrati in cloud

Lotto/Servizio	ID	Indicatori
	PCL2.3 PCL3.3 PCL4.3 PCL5.3 PCL6.3	• Layer SERVIZI: ✓ % di servizi migrati in cloud rispetto a quelli esistenti e oggetto di assessment.
LOTTI 7-11 SERVIZI DI SOLUTION DESIGN E ARCHITECTURE • Disegno dei workload (M1.1) • Implementazione migrazione (M1.2) • Trasferimento Dati (M2.2)	PCL7.1 PCL8.1 PCL9.1 PCL10.1 PCL11.1	• Layer SERVIZI: ✓ Numero di servizi esistenti migrabili in cloud mediante re-host
	PCL7.2 PCL8.2 PCL9.2 PCL10.2 PCL11.2	• Layer SERVIZI: ✓ Numero di servizi esistenti migrabili in cloud mediante re-platform
	PCL7.3 PCL8.3 PCL9.3 PCL10.3 PCL11.3	• Layer SERVIZI: ✓ Numero di servizi esistenti migrabili in cloud mediante re-purchase
	PCL7.4 PCL8.4 PCL9.4 PCL10.4 PCL11.4	• Layer INFRASTRUTTURE: ✓ Riduzione % di RAM/CPU/Storage disponibile post-migrazione mediante re-purchase
	PCL7.5 PCL8.5 PCL9.5 PCL10.5 PCL11.5	• Layer DATI: ✓ Numero di basi di dati migrati.

Tabella 11 - Indicatori Specifici Public cloud IaaS e PaaS

7.2.3 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA SERVIZI APPLICATIVI IN OTTICA CLOUD

Gli indicatori di seguito riportati rappresentano la "specializzazione" di secondo livello degli indicatori applicata ai Contratti Esecutivi identificati come "ad alta rilevanza" secondo i parametri riportati per la Gara strategica Servizi applicativi in ottica cloud nel presente documento.
Modalità e periodicità di misura si intendono dettagliati nei documenti per la stipula dei contratti esecutivi.

Lotto/Servizio	ID	Indicatori
Tutti (tranne PMO)	SAC.1	1. Miglioramento servizi digitalizzati: nr servizi al cittadino-impresa digitalizzati/nr di servizi che richiedono interazione con il cittadino/imprese
	SAC.2	2. Miglioramento dell'esperienza del cittadino/impresa dei sistemi applicativi realizzati/modificati
	SAC.3	3. Standardizzazione strumenti per la generazione e diffusione dei servizi digitali: % componenti di navigazione e interfaccia standard ed usabili /totale componenti
	SAC.4	4. Riusabilità – co-working soluzioni applicative realizzate e/o adottate: nr di progetti in riuso o co-working /nr totale dei progetti di digitalizzazione ove è applicabile il riuso o co-working
	SAC.5	5. Innalzamento livello di interoperabilità: numero di progetti conformi alle linee guida di interoperabilità e nel rispetto del ONCE ONLY principle /Nr progetti realizzati
	SAC.6	6. Potenziamento infrastrutture IT- adozione sistematica del paradigma cloud: nr di progetti conformi al paradigma cloud/totale di progetti realizzati
	SAC.7	7. Utilizzo piattaforme abilitanti: nr di progetti che integrano Piattaforme Abilitanti/nr progetti ove è applicabile un'integrazione con le Piattaforme Abilitanti

Tabella 12 - Indicatori Specifici Servizi Applicativi in ottica cloud

7.2.4 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA DATA MANAGEMENT

Servizio	ID	Indicatori
DATA WAREHOUSE E BUSINESS INTELLIGENCE LA.DW.1 - Sviluppo e manutenzione evolutiva di software ad hoc LA.DW.2 - Parametrizzazione e personalizzazione di soluzioni commerciali LA.DW.3 - Gestione applicativa e basi dati LA.DW.4 - Manutenzione correttiva LA.DW.5 - Manutenzione adeguativa LA.DW.6 - Supporto specialistico	DMDWBI.1	• Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive
	DMDWBI.2	• Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili
	DMDWBI.3	• Presenza di flussi di Integrazione/Scambio dati con PDND
	DMDWBI.4	• Presenza di flussi di Integrazione/Scambio dati con basi dati di interesse nazionale
	DMDWBI.5	• Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it
	DMDWBI.6	• Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID
BIG DATA / ANALYTICS LA.BD.1 - Valutazione e analisi dei dati LA.BD.2 - Acquisizione dati LA.BD.3 - Realizzazione del modello di analisi LA.BD.4 - Conduzione della soluzione di analisi	DMBDA.1	• Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive
	DMBDA.2	• Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili
	DMBDA.3	• Presenza di flussi di Integrazione/Scambio dati con PDND
	DMBDA.4	• Presenza di flussi di Integrazione/Scambio dati con basi dati di interesse nazionale
	DMBDA.5	• Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it
	DMBDA.6	• Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID
OPEN DATA LA.OD.1 - Analisi dei dati LA.OD.2 - Produzione e metadatazione di dati a livello 3A.OD.3 - Produzione di dati di livello 4 e 5 LA.OD.4 - Pubblicazione dataset	DMOD.1	• Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive
	DMOD.2	• Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili
	DMOD.3	• Open Data: n° dataset pubblicati

Servizio	ID	Indicatori
LA.OD.5 - Aggiornamento e conservazione dataset	DMOD.4	• Presenza di flussi di Integrazione/Scambio dati con PDND
	DMOD.5	• Presenza di flussi di Integrazione/Scambio dati con basi dati di interesse nazionale
	DMOD.6	• Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it
	DMOD.7	• Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID
ARTIFICIAL INTELLIGENCE/MACHINE LEARNING LA.AI.1 - Supporto specialistico	DMAIML.1	• Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive
	DMAIML.2	• Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili
	DMAIML.3	• Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it
	DMAIML.4	• Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID

Tabella 13 - Indicatori specifici Data Management

7.2.5 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LE GARE DI SICUREZZA

Per le gare di Sicurezza[29] è previsto l'indicatore specifico di digitalizzazione ***denominato indicatore di progresso***: per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID (e successive modifiche e integrazioni), sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di prodotti e/o servizi previsti nell'Ordinativo), come di seguito riportato:

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		

Tabella 14 - Indicatore di progresso

[29] *Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni* (ID 2367); *Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni* (ID 2174); *Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni* (ID 2296)

7.2.6 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LE GARE STRATEGICHE IN PREDISPOSIZIONE

Per tutte le altre gare strategiche in predisposizione e/o pubblicazione gli indicatori saranno definiti in documentazione di gara o comunque entro la stipula, compatibilmente con i tempi di pubblicazione delle stesse.

7.3 INDICATORI II LIVELLO PER CONTRATTI AD ALTA RILEVANZA

7.3.1 INDICATORI SPECIFICI DI DIGITALIZZAZIONE DI II LIVELLO PER LA GARA STRATEGICA DIGITAL TRANSFORMATION

Non previsti.

7.3.2 INDICATORI SPECIFICI DI II LIVELLO PER LA GARA STRATEGICA PUBLIC CLOUD IAAS E PAAS

Non previsti.

7.3.3 INDICATORI SPECIFICI DI II LIVELLO PER LA GARA STRATEGICA SERVIZI APPLICATIVI IN OTTICA CLOUD

IDI	Indicatore di I livello	IDII	Indicatore di II livello
SAC.1	1. Miglioramento servizi digitalizzati: nr servizi al cittadino-impresa digitalizzati/nr di servizi che richiedono interazione con il cittadino/imprese	SAC.1a	• Numero di modelli standard di sviluppo web disponibili tramite Designers Italia che l'Amministrazione intende adottare
		SAC.1b	• Numero di processi operativi/procedure re-ingegnerizzati in ottica di semplificazione mediante la transizione al digitale
		SAC.1c	• Numero di servizi migrati da analogico a digitale
SAC.2	2. Miglioramento dell'esperienza del cittadino/impresa dei sistemi applicativi realizzati/modificati	SAC.2a	• Numero di servizi digitali monitorati tramite Web Analytics Italia (solo per servizi di gestione)
		SAC.2b	• Numero di modelli standard di sviluppo web disponibili tramite Designers Italia che si prevede di adottare
		SAC.2c	• Numero di test di usabilità previsti dalle Linee Guida AGID per il design dei servizi effettuati

IDI	Indicatore di I livello	IDII	Indicatore di II livello
		SAC.2d	• Numero di siti per i quali è stato rilevato il livello di conformità secondo le Linee guida AgID sull'accessibilità degli strumenti informatici
SAC.3	3. Standardizzazione strumenti per la generazione e diffusione dei servizi digitali: % componenti di navigazione e interfaccia standard ed usabili /totale componenti	SAC.3a	• Numero di software open source presente su Developers Italia riutilizzato
		SAC.3b	• Numero di software open source pubblicato su Developers Italia
SAC.4	4. Riusabilità – co-working soluzioni applicative realizzate e/o adottate: nr di progetti in riuso o co-working /nr totale dei progetti di digitalizzazione ove è applicabile il riuso o co-working	SAC.4a	• Numero di API registrate nel Catalogo
		SAC.4b	• Numero di API fruite tramite il Catalogo
		SAC.4c	• Numero di servizi digitali per l'interazione erogati dalle PAC ad altre amministrazioni
		SAC.4d	• Numero di servizi digitali che utilizzano API registrate nel Catalogo
SAC.5	5. Innalzamento livello di interoperabilità: numero di progetti conformi alle linee guida di interoperabilità e nel rispetto del ONCE ONLY principle/Nr progetti realizzati	SAC.5a	• Numero di servizi digitali esistenti on-premise migrati verso servizi cloud qualificati;
		SAC.5b	• Numero di nuovi servizi digitali realizzati utilizzando servizi cloud qualificati;
SAC.7	7. Utilizzo piattaforme abilitanti: nr di progetti che integrano Piattaforme Abilitanti/nr progetti ove è applicabile un'integrazione con le Piattaforme Abilitanti	SAC.7°	• numero di documenti digitalizzati confluiti nel FSE (referti di medicina di laboratorio e ricette)
		SAC.7b	• Percentuale di prenotazioni effettuate online rispetto al totale
		SAC.7c	• Numero di servizi offerti da NoiPA utilizzati
		SAC.7d	• numero di autenticazioni fatte con SPID e CIE ai servizi online della PA
		SAC.7e	• numero di servizi digitali accessibili tramite SPID e CIE
		SAC.7f	• numero di servizi digitali integrati con PagoPA
		SAC.7g	• numero di servizi digitali integrati con l'App IO

IDI	Indicatore di I livello	IDII	Indicatore di II livello
		SAC.7h	• numero di servizi digitali integrati con l'INAD
		SAC.7i	• numero di Musei accreditati al Sistema Museale Nazionale.

Tabella 15 - Indicatori specifici II livello Servizi Applicativi in ottica cloud

7.3.4 INDICATORI SPECIFICI DI II LIVELLO PER LA GARA STRATEGICA DATA MANAGEMENT

IDI	Indicatore di I livello	IDII	Indicatore di II livello
DMDWBI.1	Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive	DMDWBI.1a	• numero di dataset che adottano un'unica licenza aperta identificata a livello nazionale
		DMDWBI.1b	• numero di basi dati di interesse nazionale che espongono API coerenti con il modello di interoperabilità e con i modelli di riferimento di dati nazionali ed europei
		DMDWBI.1c	• numero di altre PP.AA. coinvolte
DMOD.3	Open Data: n° dataset pubblicati	DMOD.3a	• numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalla Direttiva (UE) 2019/1024
		DMOD.3b	• numero di dataset resi disponibili attraverso i servizi di dati territoriali di cui alla Direttiva 2007/2/EC (INSPIRE)
		DMOD.3c	• numero di dataset con metadati di qualità conformi agli standard di riferimento europei e dei cataloghi nazionali
		DMOD.3d	• numero di dataset aperti conformi ad un sottoinsieme di caratteristiche di qualità derivate dallo standard ISO/IEC 25012
		DMOD.3e	• numero di dataset che adottano un'unica licenza aperta identificata a livello nazionale

Tabella 16 - Indicatori specifici II Data Management

- Fine del documento -

ALLEGATO H – REGOLAMENTO DEGLI ORGANISMI DI COORDINAMENTO E CONTROLLO

consip

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

AGID Agenzia per l'Italia Digitale

Piano Strategico ICT
Governance delle Gare Strategiche

Organismi di coordinamento e controllo

Regolamento

Sommario

1. PREMESSA

Il presente documento raccoglie le modalità di funzionamento degli Organismi di coordinamento e controllo deputati alla governance delle Gare afferenti al Piano Strategico ICT 2019[1], elaborato da AgID con il supporto di Consip e definisce la parte di attività, compiti e responsabilità comuni a tutte le Gare Strategiche, rimandando ai documenti integrativi specifici e/o alle prescrizioni di dettaglio contenute nella documentazione di gara di ciascuna Gara Strategica, per tutti gli aspetti peculiari per i quali non è possibile un funzionamento unitario.
Il regolamento potrà essere rivisto su iniziativa di AgID, Consip o del Dipartimento per la trasformazione digitale.

2. DEFINIZIONI

- **Gara Strategica:** iniziativa di acquisizione afferente al Piano Strategico ICT 2019 e sue evoluzioni. In particolare:
  - Digital Transformation (ID 2069),
  - Public Cloud IaaS e PaaS (ID 2213),
  - Servizi Applicativi in ottica cloud (ID 2212),
  - Data Management (ID 2102),
  - Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367),
  - Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174),
  - Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)[2],
  - Sanità digitale 1 - sistemi informativi clinico assistenziali (ID 2202),
  - Sanità digitale 2 - sistemi informativi sanitari e servizi al cittadino (ID 2365),
  - Sanità digitale 3 - sistemi informativi gestionali (ID 2366),
  - Public Cloud SaaS[3].

[1] Comprensivo delle sue evoluzioni.
[2] ID 2296 è bandita ai sensi dell'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, che ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, 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". Per la merceologia trattata è considerata al pari delle gare strategiche.
[3] Tutte le gare che saranno definite.

- **Organismi di coordinamento e controllo**: differenziati in Organismo tecnico e Organismo strategico, sono le Strutture deputate alla governance dell'esecuzione dei Contratti derivanti dalle Gare Strategiche.
- **Organismo tecnico di coordinamento e controllo**: struttura organizzativa, nominata per ciascuna Gara, altresì definito **Comitato Tecnico**. È composto da rappresentanti istituzionali di **AgID e Consip**, anche integrati con altri soggetti terzi da questi individuati e da rappresentanti del Fornitore/dei Fornitori aggiudicatari della specifica procedura di gara (Gara Strategica).
- **Organismo Strategico di coordinamento e controllo**: struttura organizzativa unica, altresì definita **Comitato Strategico**, per la governance di tutte le gare strategiche del Piano ICT 2019, composta da rappresentanti istituzionali di AgID, Consip e dal Dipartimento per la Trasformazione digitale, individuati dai medesimi soggetti.
- **Componente pubblica del Comitato Tecnico**: i rappresentanti di AgID e Consip.
- **Fornitore**: operatore economico aggiudicatario della procedura relativa ad una Gara Strategica.

3. REGOLAMENTO INTERNO PER IL FUNZIONAMENTO DELL'ORGANISMO TECNICO DI COORDINAMENTO E CONTROLLO

3.1 PRINCIPI GENERALI

1. Viene istituito un Comitato Tecnico per ogni Gara Strategica funzionale a tutti i Lotti della medesima Gara;
2. Partecipano al Comitato: AgID, Consip e i fornitori di ciascun Lotto di gara. I rappresentanti degli operatori economici aggiudicatari delle Gare Strategiche hanno diritto a partecipare alle attività del Comitato stesso come di seguito disciplinato;
3. I componenti del Comitato tecnico sono così individuati:
   - ✓ 2 rappresentanti per conto di AgID. Tali rappresentanti possono essere sostituiti mediante delega di AgID da altri rappresentanti (sempre nel numero massimo di 2);
   - ✓ 2 rappresentanti per conto di Consip. Tali rappresentanti possono essere sostituiti mediante delega di Consip da altri rappresentanti (sempre nel numero massimo di 2);
   - ✓ 1 rappresentante per conto dell'/gli aggiudicatario/i di ogni Lotto della Gara Strategica di riferimento. Nel caso in cui il fornitore sia costituito da un RTI, il rappresentante designato dovrà fare capo alla mandataria. Qualora, nell'ambito della documentazione relativa alla specifica Gara Strategica, siano attribuiti al RUAC specifici compiti di interfacciamento con gli organismi di coordinamento e controllo, tale rappresentante dovrà coincidere con il RUAC. In ogni caso, ogni aggiudicatario dovrà indicare anche il nominativo di un supplente (sempre facente capo alla mandataria, in caso di RTI). Il rappresentante (e il supplente) dovranno essere dotati di poteri di rappresentanza dell'azienda;
4. Il Comitato si riunirà almeno quadrimestralmente e comunque, nelle modalità descritte nel presente documento, ogni qualvolta AgID/Consip ne ravvedano la necessità;
5. Il Comitato potrà essere convocato sia relativamente a tematiche riguardanti un singolo Lotto sia per tematiche riguardanti più Lotti; in ogni caso saranno convocati tutti i soggetti dei Lotti coinvolti;
6. Il Comitato potrà coinvolgere qualora necessario una o più Amministrazioni beneficiarie dei contratti derivanti dalla Gara Strategica o soggetti istituzionali competenti su specifiche tematiche.

3.2 COMPITI E RESPONSABILITÀ DEL COMITATO TECNICO

Si riportano di seguito le attività e le responsabilità in capo al Comitato Tecnico, fermo restando quanto previsto nella documentazione relativa a ciascuna specifica Gara Strategica:

1. monitorare la coerenza dell'impiego dei servizi/forniture messi a disposizione dai diversi Lotti rispetto all'oggetto e al perimetro della Gara Strategica di riferimento e ai vincoli normativi;
2. monitorare il rispetto dei vincoli contrattuali e la qualità della Fornitura;
3. monitorare lo stato di avanzamento dell'Accordo Quadro, in termini di numero di contratti, dimensione degli stessi e massimale complessivo eroso, tramite analisi e approfondimento periodici delle informazioni rese disponibili dal fornitore e prodotti tramite:

a) formati di office automation fruibili dai componenti del Comitato afferenti a Consip e AgID (esclusi pdf),
b) link ad aree riservate dei portali di fornitura, con possibilità di download dei contenuti,
c) altri strumenti messi a disposizione dal Fornitore e/o dai soggetti istituzionali coinvolti nella Governance.

Le informazioni rese disponibili dal Fornitore dovranno contenere almeno il seguente dettaglio minimo:

a) informazioni tecnico/economiche relative a tutti i contratti esecutivi stipulati con le Amministrazioni; in particolare, dovrà essere disponibile la vista per Amministrazione contenente il dettaglio dei servizi acquistati, con il relativo massimale impegnato ed il consuntivo alla data; tali informazioni dovranno essere rese disponibili mensilmente, entro il 15 del mese successivo al mese di riferimento.
b) report descrittivi delle iniziative progettuali con periodicità quadrimestrale, resi disponibili almeno 15 giorni lavorativi prima della riunione del Comitato; in particolare per ciascuna Amministrazione si dovrà fornire: una descrizione di massima dell'iniziativa con i relativi obiettivi, eventuale ricorso a soluzioni in riuso (motivando i casi in cui i processi/le soluzioni sviluppate si sono differenziate da pregresse analoghe), eventuale partecipazione di più Amministrazioni al medesimo progetto in modalità di co-working o co-partecipazione finanziaria;

Nel caso in cui la documentazione di gara di ciascuna specifica Gara Strategica preveda informazioni di maggior dettaglio rispetto a quanto sopra descritto, il Fornitore comunque dovrà rendere disponibili al Comitato almeno le viste aggregate che consentano di reperire le informazioni sopra descritte.

Relativamente alla documentazione di cui ai punti precedenti, il Comitato ha facoltà di richiedere al fornitore informazioni aggiuntive/integrative a quelle prodotte.

Si precisa inoltre che la documentazione prodotta dovrà essere resa disponibile anche ai componenti del Comitato Strategico, ove richiesto.

4. analizzare i progetti implementati da Amministrazioni diverse nell'ambito degli stessi Accordi Quadro, nei casi specifici, identificati da Consip/AgID o segnalati dalle Amministrazioni, in cui si evidenzino analogie funzionali, tecniche, di obiettivo;
5. analizzare le proposte di standardizzazione di processi, modelli, soluzioni, metriche, metodologie di stima dei servizi e, nella sua componente pubblica, valutarne l'adozione, in accordo con il Comitato Strategico;
6. valutare le eventuali proposte di evoluzione e/o adeguamento dei servizi o delle forniture da parte del fornitore, laddove espressamente previsto in documentazione di gara e con le procedure definite ad integrazione del presente regolamento;
7. monitorare ed eventualmente aggiornare i Livelli di Servizio derivanti da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o derivanti dall'ottimizzazione della rilevazione dei singoli indicatori di qualità;
8. monitorare l'andamento degli indicatori di digitalizzazione definiti nella documentazione contrattuale, quelli aggiunti dal Comitato Strategico e quelli aggiuntivi eventualmente offerti dal

Fornitore, anche attraverso eventuali strumenti messi a disposizione dal fornitore e/o dai soggetti istituzionali coinvolti nella Governance;

9. su richiesta dell'Amministrazione, o per contratti di alta rilevanza segnalati dall'Organismo Strategico di Coordinamento e Controllo, il Comitato Tecnico potrà:
    a) esaminare specifici Contratti Esecutivi, comprensivi dei relativi allegati (ad esempio Piano dei Fabbisogni, Piano Operativo, etc.);
    b) dialogare, se necessario, con l'Amministrazione coinvolta e/o il Fornitore di riferimento per l'acquisizione di ulteriori informazioni o l'approfondimento di specifiche tematiche funzionali e/o tecnologiche;
    c) segnalare all'Amministrazione eventuali criticità/punti di attenzione;
    d) verificare gli obiettivi raggiunti e il loro eventuale scostamento rispetto al target prefissato;
10. segnalare al Comitato Strategico progetti con elevata potenzialità di riuso da parte di altre Amministrazioni, anche indicati dalle Amministrazioni o dai fornitori;
11. richiedere l'intervento del Comitato Strategico (cd. escalation):
    a) per eventuali criticità rilevate sui contratti esecutivi ad alta rilevanza[4] relativi a progetti speciali e/o di rilevanza nazionale e/o strategici e/o relativi alle piattaforme abilitanti, realizzati o implementati con le gare strategiche;
    b) in merito ai rapporti con le Amministrazioni e/o i Fornitori;
    c) in relazione a tutti i punti precedenti.
12. svolgere qualsiasi altra funzione ad esso attribuita dalla documentazione contrattuale relativa alla specifica Gara Strategica;
13. valutare e fornire indicazioni ai fornitori, sentito anche il Comitato Strategico, in merito alla necessità di un eventuale adeguamento alle eventuali evoluzioni della normativa tecnica di settore, per quanto compatibile con la documentazione contrattuale relativa alle singole Gare Strategiche.

Per ciascuna Gara Strategica, AgID e Consip, inoltre, valuteranno la predisposizione, all'avvio delle attività dello specifico Comitato Tecnico, di integrazioni al presente regolamento, al fine di regolarne gli aspetti peculiari (es. revisione listini).

Ogni decisione del Comitato si intende validamente assunta se condivisa dai rappresentanti di AgID e Consip. In ogni caso, ogni decisione deve essere previamente comunicata (anche a mezzo di PEC, qualora non presenti alla seduta) a tutti i rappresentanti dei fornitori cui si riferiscono le decisioni assunte (o per Lotti o per merito). I rappresentanti dei fornitori dei Lotti interessati dalla decisione in oggetto hanno altresì diritto di prendere visione degli atti del Comitato, salvo le previsioni di legge in materia, nonché di presentare memorie scritte e documenti, che il Comitato ha l'obbligo di valutare ove siano pertinenti all'oggetto della discussione.

Le decisioni sono assunte nelle forme e nei modi stabiliti da AgID e Consip.

[4] Secondo i criteri definiti per ciascuna Gara Strategica

3.3 INDIVIDUAZIONE DEL PRESIDENTE - RIUNIONI DEL COMITATO TECNICO

1. Il ruolo di Presidente del Comitato è ricoperto da un rappresentante di AgID.
2. Le riunioni del Comitato sono convocate dal Presidente o da persona da lui designata, con almeno 5 giorni solari di preavviso, di norma tramite messaggi di posta elettronica certificata (PEC). La nota di convocazione dà indicazione dell'ordine del giorno, che è definito dal Presidente anche sulla base delle proposte, esigenze o richieste espresse da ciascuna parte rappresentata nel Comitato o dalle Amministrazioni. Alla nota di convocazione è allegata eventuale documentazione rilevante ai fini degli argomenti all'ordine del giorno.
3. In funzione degli argomenti trattati, ciascuna parte rappresentata potrà chiamare a partecipare alle riunioni proprio personale di supporto, nel numero massimo di 2 ulteriori persone oltre ai rappresentanti già previsti.
4. Ai fini della validità delle riunioni è necessario che siano presenti almeno i rappresentati di AgID e Consip e, contestualmente, i fornitori in numero pari alla maggioranza dei fornitori del/i Lotto/i cui si riferisce l'oggetto della riunione.
5. Nel caso in cui non sia raggiunta la validità della seduta, viene riconvocata una nuova seduta che ha validità anche con la sola presenza dei rappresentanti di AgID e Consip.

3.4 ATTI DEL COMITATO TECNICO

1. Gli argomenti discussi nel corso delle riunioni e le decisioni assunte risultano da apposito verbale.
2. Il verbale, redatto dal segretario nominato all'inizio della riunione, è trasmesso in versione preliminare a mezzo posta elettronica a tutti i componenti. La funzione di segretario dovrà essere ricoperta da un rappresentante di AgID o di Consip.
3. I rappresentanti dei Fornitori, presenti alla riunione, hanno facoltà di proporre modifiche o integrazioni nei tempi indicati nella nota di trasmissione, trascorsi i quali senza che nessuna richiesta di modifica sia stata comunicata al segretario e trasmessa per conoscenza a tutti i componenti, il verbale si intende approvato.
4. Le modifiche e integrazioni sono accolte a discrezione di AgID e Consip.
5. L'approvazione del verbale in versione definitiva, a seguito di richieste di modifiche o integrazioni, è comunicata da ciascun componente presente alla riunione a mezzo posta elettronica, salvo quanto previsto ai punti precedenti. A seguito dell'approvazione secondo le modalità sopra indicate, il verbale è firmato digitalmente da AgID e Consip e per presa visione da ciascun componente presente per ogni parte rappresentata ed inviato a mezzo PEC da AgID, con i relativi eventuali allegati, a tutti i componenti. Per esigenze di necessità ed urgenza o comunque per ragioni di interesse pubblico o di norme specifiche, AgID o Consip possono decidere di approvare il verbale anche senza le modifiche/integrazioni proposte dai fornitori.
6. AgID e Consip, in relazione agli argomenti trattati, stabiliscono le forme di pubblicità dei verbali e dei documenti allegati.

4. REGOLAMENTO INTERNO PER IL FUNZIONAMENTO DELL'ORGANISMO TRATEGICO DI COORDINAMENTO E CONTROLLO

4.1 PRINCIPI GENERALI

1. Viene istituito un Comitato Strategico per la governance delle gare strategiche, col fine di garantire l'allineamento complessivo dei contratti e dei progetti rispetto al Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022 (e sue successive edizioni), rispetto alle linee guida AgID e alle best practices da quest'ultima individuate ed in coerenza con le previsioni del PNRR.
2. Il Comitato Strategico è così composto:
   - ✓ 1 rappresentante per conto di AgID;
   - ✓ 1 rappresentante per conto di Consip;
   - ✓ 1 rappresentante per conto del Dipartimento per la trasformazione digitale.

4.2 COMPITI E RESPONSABILITÀ DEL COMITATO STRATEGICO

Si riportano di seguito le attività e le responsabilità in capo al Comitato Strategico, fermo restando quanto previsto nella documentazione relativa a ciascuna specifica Gara Strategica:

1. definire l'indicatore del Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022 *"R.A.8.1d - Incremento del livello di trasformazione digitale mediante l'utilizzo dei servizi previsti dalle Gare strategiche*", in particolare, dovrà:
   a) costruire il livello base dell'indicatore nel 2021, utilizzando un sistema pesato degli indicatori di digitalizzazione delle Gare Strategiche e individuare il valore target per l'anno 2022, nonché gli incrementi attesi annualmente per gli anni successivi;
   b) a partire dal 2022, con periodicità almeno annuale, raccogliere le misure relative agli indicatori pertinenti e al valore dell'indicatore R.A.8.1d.

   Si precisa che alle Gare Strategiche relative alla sicurezza si applica l'indicatore specifico denominato *Indicatore di progresso* nelle modalità definite in documentazione di gara;
2. produrre linee di indirizzo strategico per le Gare Strategiche attive, in predisposizione e per nuove gare volte a soddisfare esigenze di natura strategica, indirizzate nel Piano Triennale per l'informatica o nel PNRR;
3. valutare, trasversalmente a più Gare Strategiche e ai relativi contratti, il livello di aderenza rispetto alle linee strategiche;
4. valutare la coerenza strategica dei contratti esecutivi identificati come *ad alta rilevanza*, risultanti da rilevazioni proprie o segnalati dai Comitati Tecnici o ancora dalle Amministrazioni beneficiarie dei suddetti contratti;
5. garantire la disponibilità di misure (procedurali e/o strumentali) per l'allineamento informativo tra i soggetti coinvolti a vario titolo nelle attività relative alle Gare Strategiche (Comitati Tecnici, Amministrazioni, Fornitori, etc.);

6. valutare ed eventualmente ratificare le proposte di standardizzazione di processi, modelli, soluzioni, metriche, metodologie di stima dei servizi, formulate dai Comitati Tecnici, nel caso di impatti trasversali a più gare strategiche;
7. prendere atto della modalità di revisione dei prezzi e di remunerazione dei servizi, laddove previsto dalla documentazione di gara e formulate secondo le procedure definite ad integrazione del presente regolamento;
8. avviare indagini di soddisfazione delle Amministrazioni per i servizi erogati nell'ambito delle iniziative strategiche, raccogliendone e divulgandone gli esiti;
9. promuovere il riuso di soluzioni e processi tra Amministrazioni, anche avvalendosi delle segnalazioni dei Comitati Tecnici;
10. gestire le escalation segnalate dai Comitati Tecnici.

4.3 RIUNIONI DEL COMITATO STRATEGICO

1. Il Comitato si riunirà almeno semestralmente;
2. la convocazione potrà essere fatta da uno qualunque dei rappresentanti sopra indicati;
3. la riunione del Comitato Strategico è valida se sono presenti tutti i rappresentanti sopra riportati e prevede la nomina, all'inizio della seduta, di un segretario, cui spetterà la verbalizzazione e le relative attività di invio;
4. nelle riunioni periodiche il Comitato Strategico potrà coinvolgere, al bisogno, una o più Amministrazioni beneficiarie o soggetti istituzionali competenti su specifiche tematiche e/o uno o più fornitori aggiudicatari delle Gare Strategiche.

4.4 ATTI DEL COMITATO STRATEGICO

1. Gli argomenti discussi nel corso delle riunioni e le decisioni assunte risultano da apposito verbale;
2. il verbale, redatto dal segretario nominato all'inizio della riunione, è trasmesso in versione preliminare a mezzo posta elettronica a tutti i componenti. La funzione di segretario dovrà essere ricoperta da un rappresentante di AgID o di Consip;
3. ogni decisione del Comitato si intende valida se assunta all'unanimità dai rappresentanti di AgID, Consip e del Dipartimento per la trasformazione digitale;
4. fatte salve le indicazioni di legge sulla trasparenza, AgID, Consip e il Dipartimento per la trasformazione digitale, in relazione agli argomenti trattati, stabiliranno le forme di pubblicità degli atti e dei documenti relativi alla governance delle Gare strategiche di volta in volta adottati, ivi incluse ad es. pubblicazioni su siti istituzionali, circolari, studi, etc.

- fine del documento -

ALLEGATO I – CONTRATTO DI AVVALIMENTO

ACCORDO DI AVVALIMENTO

TRA

Capgemini Italia S.p.A. con sede legale in Roma (RM), Via di Torre Spaccata n. 140, cap 00173, Codice Fiscale 10365640159 e Partita IVA 04877961005 ed iscrizione al Registro delle Imprese di Roma al n. 10365640159 in data 19/02/1996, rappresentata per la sottoscrizione del presente Accordo dal Dott. Andrea Falleni, nato a Bologna (BO) il 22 settembre 1968 C.F. FLLNDR68P22A944C , domiciliato per la carica presso la sede societaria ove appresso, nella sua qualità di Amministratore Delegato e legale rappresentante**,** di seguito denominata per brevità " Capgemini " o "Ausiliaria"

E

Intellera Consulting S.r.l. con sede legale in Milano, Piazza Tre Torri n. 2, codice fiscale, Partita IVA ed iscrizione al Registro delle Imprese di Milano-Monza-Brianza-Lodi n. 11088550964, R.E.A. n. 2579362, rappresentata per la sottoscrizione del presente accordo da **Giancarlo Senatore** nato a Cava De' Tirreni (SA) il 07/02/1966, residente in Via Adriano I° n. 72 - 00167 Roma (RM), Codice Fiscale SNTGCR66B07C361Q, domiciliato per la carica presso la sede societaria ove appresso nella sua qualità di Amministratore Delegato, e Legale Rappresentante, e **Mario Papini**, nato a Monza (MB) il 22/05/1969, residente in Via Carlo Meda n. 43 – 20900 Monza (MB), Codice Fiscale PPNMRA69E22F704Z, nella sua qualità di Amministratore, domiciliato per la carica presso la sede societaria di seguito denominata per brevità "Concorrente" o "Intellera";
(di seguito anche denominate congiuntamente "le Parti", o singolarmente "la Parte")

Premesso che

1. Consip S.p.A. (di seguito per brevità anche "Consip" o "Ente Appaltante" o "Stazione Appaltante") ha indetto una "*Gara a Procedura Aperta ai sensi Del D.Lgs. 50/2016 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto L'affidamento di Servizi di Sicurezza da remoto, di Compliance e Controllo per le Pubbliche Amministrazioni - ID 2296 - CIG Lotto 2 8884642E81*" mediante Bando di gara pubblicato sulla GUUE N° S 143 del 27/07/2021 (di seguito per brevità "Gara");

2. Le Parti intendono partecipare alla Gara in costituendo Raggruppamento Temporaneo di Imprese ("RTI") unitamente alla società HSPI S.p.A. e Teleconsys S.p.A., Intellera svolgerà il ruolo di mandataria-capogruppo;

3. Capgemini è in possesso del requisito previsto al punto 7.2 lett. c) del Capitolato d'oneri, e precisamente *"fatturato specifico medio annuo per Servizi di compliance e controllo (servizi inerenti la sicurezza ICT)" riferito agli ultimi due esercizi finanziari disponibili, ovverosia approvati, alla data di scadenza del termine per la presentazione delle offerte, non inferiore ad € 1.312.500,00, IVA esclusa".*

4. Scopo del presente Accordo è dato dall'interesse di Intellera a partecipare alla gara di cui al precedente punto 1) in qualità di mandataria-capogruppo avvalendosi dei requisiti in eccedenza di Capgemini, considerata la carenza in capo a Intellera della quota maggioritaria dei requisiti di cui al precedente punto 3).

per tutto quanto sopra premesso, le Parti convengono quanto segue:

Art. 1 – Premesse

1.1 Le Premesse sono parte integrante e sostanziale del presente Accordo.

Art. 2 – Oggetto dell'Accordo

2.1 Con il presente Accordo Capgemini si obbliga a mettere a disposizione di Intellera e verso l'Ente Appaltante il proprio know how, le proprie tecnologie e risorse, riferibili al requisito di cui al punto 3) delle premesse, in conformità a quanto previsto dall'Art. 89 del Decreto Legislativo 18 aprile 2016, n. 50 e s.m.i.

2.2 In particolare, con il presente Accordo Capgemini si obbliga nei confronti di Intellera e dell'Ente Appaltante a mettere a disposizione, per tutta la durata dell'appalto, il seguente fatturato specifico: **fatturato specifico medio annuo** per *"Servizi di compliance e controllo (servizi inerenti la sicurezza ICT)"* realizzato negli ultimi due esercizi finanziari disponibili alla data di presentazione delle offerte (2019 – 2020) pari ad Euro 325.000,00 (650.000,00 totali nel biennio), IVA esclusa;

Ai suddetti fini, per tutta la durata dell'appalto, Capgemini metterà a disposizione strutture, risorse qualificate, nonché mezzi afferenti la propria struttura aziendale come di seguito meglio specificati:

le risorse professionali specialistiche con competenze specifiche connesse al predetto requisito riportate di seguito:

- ✓ Information security expert
- ✓ Security compliance manager
- ✓ Business continuity specialist
- ✓ Data protection specialist
- ✓ IT risk manager
- ✓ Security strategist

i mezzi e metodologie a supporto per la realizzazione di quanto sopra come di seguito riportate:

- ➢ Security strategy
- ➢ Vulnerability assessment
- ➢ Security Assessment and Remediation
- ➢ Penetration testing e validation
- ➢ Compliance normativa e data protection

- Governance risk and compliance
- Risk mitigation
- Cyber Risk Quantification
- Analisi e gestione degli incidenti
- Business continuity management

2.3 Con la sottoscrizione del presente contratto, l'Ausiliaria assume la responsabilità solidale con il Concorrente nei confronti della Stazione Appaltante, in relazione alle prestazioni oggetto del Contratto.

Art. 3 – Durata e corrispettivo

3.1 Il presente Accordo decorrerà dalla data della sua sottoscrizione ed avrà efficacia per tutta la durata dell'appalto di cui al punto 1) delle premesse, dalla data dell'eventuale stipula del Contratto d'appalto e fino alla conclusione dello stesso e, in ogni caso, sino all'estinzione di tutte le obbligazioni pendenti tra le Parti e/o nei confronti dell'Ente Appaltante in base al Contratto d'appalto.
3.2 Il presente Accordo si intenderà risolto a tutti gli effetti tra le Parti, senza bisogno di ulteriori formalità o adempimenti, col verificarsi di uno qualunque dei seguenti eventi:
- alla data in cui le Parti avranno notizia della aggiudicazione della Gara da parte dell'Ente Appaltante ad altra impresa ovvero ad altro soggetto giuridico diverso dal RTI;
- alla data dell'eventuale annullamento, in via definitiva e non soggetta ad impugnativa, della procedura di Gara;
- nel caso di aggiudicazione della Gara al RTI, con l'approvazione del certificato di collaudo definitivo, o altro atto o certificato di natura equipollente, e comunque con la liquidazione di tutte le pendenze, tra l'Ente Appaltante ed il RTI, ovvero qualora si verifichi altra causa di cessazione degli effetti giuridici o di estinzione del Contratto stipulato tra il RTI e l'Ente Appaltante.

Le Parti congiuntamente stabiliscono che in un separato accordo sarà fissato il corrispettivo che Intellera si impegna a corrispondere ad Capgemini in relazione alle risorse e mezzi messi a disposizione di cui all'Art. 2 del presente Accordo.

Art. 4 – Proprietà Intellettuale

4.1 Le Parti convengono sin da ora che le eventuali soluzioni tecnologiche individuate nonché le relative specifiche tecniche di quanto afferente al servizio oggetto dell'appalto, resteranno di proprietà esclusiva della Parte che ne avrà curato lo sviluppo e che pertanto sarà libera di utilizzarle e sfruttarle commercialmente a qualsiasi titolo, senza che l'altra Parte abbia nulla a pretendere, fermo restando l'obbligo eventualmente derivante da fonti normative primarie o secondarie, da regolamento e/o dal rapporto contrattuale in essere con l'Ente Appaltante di trasferire tale proprietà a terzi.
4.2 Qualora nell'ambito del presente Accordo una delle Parti abbia rivelato all'altra Parte informazioni di tipo tecnico, resta inteso che la mera comunicazione delle summenzionate informazioni, in qualsiasi forma essa avvenga (es. supporto cartaceo, informatico o altro), non comporta automaticamente alcuna variazione al regime di proprietà intellettuale, né garantisce alla Parte che apprende l'informazione, salvo diverso Accordo tra le Parti, alcun diritto di licenza.

4.3 Il presente Accordo non modifica il regime di proprietà intellettuale relativo ai singoli prodotti resi disponibili e forniti rispettivamente dalle Parti.

Art. 5- Riservatezza e Confidenzialità

5.1 In esecuzione del presente Accordo, le Parti potranno rendersi reciprocamente disponibili informazioni di carattere tecnico e/o commerciale, anche riservate e/o confidenziali. Tali informazioni saranno utilizzate dalla Parte che le apprende esclusivamente in relazione alle finalità e scopi definiti nell'oggetto del presente Accordo.

5.2 Le Parti si impegnano a rispettare - e a far rispettare ai propri dipendenti - il vincolo di riservatezza relativamente a tutte le informazioni, i dati, le documentazioni e le notizie che siano ritenute riservate - ivi comprese le informazioni relative ai criteri di produzione, vendita ed organizzazione di Capgemini e di Intellera, e che, comunque, non siano finalizzate alla pubblica diffusione.

In tal senso le Parti saranno tenute a porre in essere tutte le necessarie misure di prevenzione e, in particolare, tutte le azioni legali necessarie per evitare la diffusione e l'utilizzo delle informazioni ritenute riservate.

Le Parti si impegnano a rispettare gli obblighi di riservatezza anche successivamente alla scadenza del periodo di validità del presente Accordo per un termine di tre anni.

5.3 Qualora la diffusione presso terzi di materiale o di informazioni ritenuti riservati, sia stata causata da atti o fatti direttamente o indirettamente imputabili ad una delle Parti e/o ai rispettivi dipendenti, la stessa sarà tenuta a risarcire alla controparte gli eventuali danni che siano direttamente o indirettamente connessi alla diffusione della suddetta documentazione o materiali ritenuti riservati.

Le disposizioni normative contemplate nel presente articolo non verranno applicate qualora la Parte ritenuta inadempiente rispetto alle citate disposizioni, dimostri e documenti che:

– era già a conoscenza delle informazioni e delle documentazioni rese pubbliche, prima dell'acquisizione delle stesse in virtù dei rapporti intrattenuti con la controparte;

– le informazioni e le documentazioni relative o connesse - direttamente o indirettamente - alla esecuzione degli obblighi derivanti dal presente Accordo, siano già di pubblico dominio indipendentemente da una azione omissiva degli obblighi contrattuali contemplati nel presente articolo.

5.4 Le Parti si impegnano inoltre a garantire che i dati personali forniti da ciascuna delle Parti verranno tutelati a norma del Regolamento UE 2016/679, recante disposizioni a tutela delle persone e degli altri soggetti rispetto al trattamento dei dati personali.

Inoltre, nel rispetto della normativa antitrust le Parti sin da ora convengono che nello svolgimento delle attività disciplinate dal presente Accordo:

- nessun Accordo formale o informale, scritto od orale sarà realizzato per coordinare le rispettive attività in modo tale da precludere gli sbocchi al mercato dei concorrenti attuali o potenziali delle Parti o da ottenere una spartizione dei mercati sulle eventuali attività in concorrenza;
- nessuna informazione sensibile di mercato (quali ad esempio distribuzione territoriale dei clienti, volume e spesa per tipologia di servizio, strategie commerciali e termini di vendita e prezzi) che consenta alle Parti un loro sfruttamento nei mercati su cui le Parti sono attive ai danni della concorrenza sarà scambiata;

- nessuna attività che abbia effetto su terzi concorrenti delle Parti sarà posta in essere dalle stesse a seguito dello svolgimento di quanto disciplinato dal presente Accordo;
- nessuna ricerca e nessuno sviluppo di servizi congiuntamente condotti, per quanto oggetto del presente Accordo, potranno comunque implicare il passaggio di informazioni in possesso delle Parti circa pratiche commerciali, costi e profittabilità delle offerte o modalità di distribuzione o di esecuzione dei servizi dei concorrenti di ciascuna delle Parti.

Art. 6 - Rapporti tra le Parti

6.1 Con il presente Accordo le Parti non intendono costituire alcuna forma di joint-venture, alcuna società, anche di fatto, od altra forma di stabile organizzazione, né conferiscono diritti e/o facoltà per agire l'una in nome e per conto dell'altra né concludono un contratto di agenzia e/o distribuzione.

Art. 7 - Principi generali in materia di Rapporti Commerciali

7.1 Le Parti si impegnano al rispetto delle normative vigenti al fine di non porre in essere alcuna azione pregiudizievole nei confronti dei terzi in genere, ed in particolare dell'Ente Appaltante.
7.2 Le Parti si impegnano a porre in essere ogni azione affinché nei rapporti commerciali e di affari, si ottemperi ai seguenti principi:
a) utilizzo legittimo della immagine o nome delle Parti, senza trarne per ciascuna di esse, vantaggi commerciali non giustificati;
b) corretta gestione e uso delle informazioni riservate o confidenziali ricevute da terzi;
c) adozione di pratiche commerciali e contrattuali nel pieno rispetto dei canoni di correttezza.
7.3 In particolare le Parti, nel rispetto di quanto previsto dal D.Lgs 231/2001 dichiarano di aver già provveduto all'adozione del Modello Organizzativo richiesto da tale normativa, o si impegnano, qualora non abbiano già provveduto all'adozione del citato Modello Organizzativo, ad adottare un Modello Organizzativo che recepisca i principi di seguito evidenziati.
Per tali finalità le Parti si impegnano a svolgere le attività di propria competenza nel rispetto delle normative vigenti e dei comuni principi di etica professionale, ed in particolare all'osservanza delle seguenti forme di condotta:
- improntare la propria attività a principi di trasparenza, correttezza e lealtà;

- promuovere una competizione leale, rifuggendo e stigmatizzando il ricorso a comportamenti illegittimi o comunque scorretti per raggiungere obiettivi economici;

- perseguire l'eccellenza della performance in termini di qualità, informando i propri comportamenti a correttezza;

- mantenere con le Pubbliche Autorità locali, nazionali e sopranazionali relazioni ispirate alla piena e fattiva collaborazione, nel rispetto delle reciproche autonomie;

- non erogare contributi, vantaggi o altre utilità ai partiti politici ed alle organizzazioni sindacali, o a loro rappresentanti o candidati;

- non promettere vantaggi o altre utilità o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali;

- non effettuare spese di rappresentanza con finalità diverse dalla mera promozione dell'immagine aziendale;

- non promettere o concedere omaggi o regalie non di modico valore;

- non fornire o promettere informazioni e/o documenti riservati;

- non favorire, nei processi d'acquisto, fornitori, sub-fornitori e consulenti indicati da rappresentanti dell'Ente Appaltante;

- non esibire documenti/dati falsi od alterati;

- non tenere una condotta ingannevole che possa indurre l'Ente Appaltante in errore nella valutazione tecnico-economica dei prodotti e servizi offerti/forniti;

- non omettere informazioni dovute, al fine di orientare a proprio favore le decisioni dell'Ente Appaltante;
- non ottenere e/o modificare informazioni a vantaggio dell'azienda, accedendo in maniera non autorizzata ai sistemi informativi della Pubblica Amministrazione o abusando della posizione di fornitore della Pubblica Amministrazione;

- non corrispondere ad alcuno, direttamente o attraverso terzi -ivi comprese le imprese collegate o controllate, i propri collaboratori e consulenti- somme di denaro o altra utilità a titolo di intermediazione o simili, volte a facilitare la conclusione di determinati atti da parte della Pubblica Amministrazione;

- non versare ad alcuno, a nessun titolo, somme di denaro o altra utilità finalizzate a rendere meno onerosa l'esecuzione e/o la gestione degli affidamenti della Pubblica Amministrazione rispetto agli obblighi assunti.

Art. 8 – Controversie

8.1 Nel caso dovesse insorgere qualunque controversia nell'interpretazione e/o nell'esecuzione del presente Accordo, e quanto in esso previsto – comprese, non in via limitativa, quelle relative a questioni di validità, interpretazione, esecuzione, inadempimento, pregiudiziali e di competenza, nonché quelle inerenti l'esistenza o meno dei presupposti dell'esercizio della facoltà di risoluzione dell'Accordo stesso pattuita – le Parti si attiveranno affinchè suddetta controversia possa essere composta in via amichevole.
8.2 In caso contrario, per qualsiasi controversia che dovesse sorgere tra le Parti in merito all'interpretazione, e/o all'esecuzione del presente Accordo sarà competente in via esclusiva il Foro di Milano.

Art. 9 - Cessione e modifiche.

9.1 Qualsiasi modifica, aggiunta o cancellazione a questo Accordo sarà valida ed effettiva solo previa pattuizione scritta tra i legali rappresentanti di ciascuna delle Parti.

9.2 Le Parti non potranno cedere il presente Accordo.

Art. 10 – Comunicazioni relative all'Accordo

10.1 Tutte le comunicazioni, notizie ed informazioni saranno comunicate per iscritto tra le Parti.

Roma, 06 ottobre 2021

Firmato digitalmente da:

Capgemini Italia S.p.A. - Andrea Falleni

Intellera Consulting S.r.l. – Giancarlo Senatore – Mario Papini